DATA PROTECTION OFFICE

- TITLE:-THE CHALLENGES IMPOSED BY BIOMETRIC TECHNOLOGY ON DATA PROTECTION AND PRIVACY
- PRESENTED BY MRS DRUDEISHA CAULLYCHURN-MADHUB
- DATA PROTECTION COMMISSIONER
- PRIME MINISTER'S OFFICE
- 1.12.08

DATA PROTECTION OFFICE

THIS PRESENTATION WILL ATTEMPT TO SHOW THAT THE CHALLENGES ARE MULTI-FACETTED AND THAT THERE IS NO CLEAR AND DEFINITE ANSWER TO THE ADVANTAGES AND DISADVANTAGES OF BIOMETRIC TECHNOLOGY.

DATA PROTECTION OFFICE

WHAT IS BIOMETRIC DATA?

- Identification and verification have long been accomplished by showing **something you have**, such as a licence or a passport. Sometimes it also required **something you know**, such as a password or a PIN. As we move into a time when we need more secure and accurate measures, we begin to look at using **something you are**: biometrics.

DATA PROTECTION OFFICE

- *Biometrics* is the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences.
- The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). For our use, biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics, such as fingerprints, irises, voice patterns, facial patterns, and hand measurements, for identification and verification purposes.

DATA PROTECTION OFFICE

- **Uses of Biometrics**:
Biometrics are used in two major ways: Identification and Verification.

- *Identification* is determining who a person is. It involves taking the measured characteristic and trying to find a match in a database containing records of people and that characteristic. This method can require a large amount of processing power and some time if the database is very large. It is often used in determining the identity of a suspect from crime scene information.

DATA PROTECTION OFFICE

- *Verification* is determining if a person is who they say they are. It involves taking the measured characteristic and comparing it to the previously recorded data for that person. This method requires less processing power and time, and is often used for accessing places or information.

DATA PROTECTION OFFICE

- **How It Works**:
  Biometric devices consist of a reader or scanning device, software that converts the gathered information into digital form, and a database that stores the biometric data for comparison with previous records. When converting the biometric input, the software identifies specific points of data as match points. The match points are processed using an algorithm into a value that can be compared with biometric data in the database.

DATA PROTECTION OFFICE

- **Types of Biometrics**:
  There are two types of biometrics: behavioral and physical. Behavioral biometrics are generally used for verification while physical biometrics can be used for either identification or verification.

  Examples of physical biometrics include:

- Bertillonage - measuring body lengths (no longer used)
- Fingerprint - analyzing fingertip patterns

DATA PROTECTION OFFICE

- Facial Recognition - measuring facial characteristics
- Hand Geometry - measuring the shape of the hand
- Iris Scan - analyzing features of colored ring of the eye
- Retinal Scan - analyzing blood vessels in the eye
- Vascular Patterns - analyzing vein patterns
- DNA - analyzing genetic makeup

DATA PROTECTION OFFICE

- Examples of behavioral biometrics include:
- Speaker Recognition - analyzing vocal behavior
- Signature - analyzing signature dynamics
- Keystroke - measuring the time spacing of typed words

DATA PROTECTION OFFICE

IS BIOMETRIC DATA PERSONAL DATA?

- Biometric data **is** personal information as defined under section 2 of the DPA which provides:

"personal data" means -

data which relate to an individual who can be identified from those data; or

data or other information, including an opinion forming part of a database, whether or not recorded in a material form, about an individual whose identity is apparent or can reasonably be ascertained from the data, information or opinion;"

DATA PROTECTION OFFICE

- Biometric data is derived from an individual, is used to verify or determine a person's identity, and depending on the technology, may be a highly distinctive representation of a physiological or behavioral characteristic.

DATA PROTECTION OFFICE

IS BIOMETRIC DATA PRIVACY-NEUTRAL, PRIVACY-PROTECTIVE OR PRIVACY-INVASIVE?

- Biometrics can be deployed in a privacy-invasive fashion, in a privacy-neutral fashion, and in a privacy-protective fashion. Biometric technology is what we make it.
- Biometrics are neither a protector nor an enemy of privacy; instead, the type of deployment determines the relation between biometrics and privacy.
- The basic classifications of privacy are *personal* and *informational*.

DATA PROTECTION OFFICE

- *Personal Privacy.* For some people, the use of biometrics is seen as inherently offensive. Being required to verify one's identity through a finger-scan or voice-scan can be seen as intrusive, impersonal, or mistrustful. These objections to biometrics are based on *personal privacy*.
- *Informational Privacy.* A more common objection to biometrics is based on informational privacy; how biometric data might be misused, tracked, linked, and otherwise abused. Potential privacy-invasive misuses of biometrics are as follows:

DATA PROTECTION OFFICE

- Unnecessary or unauthorized collection – gathering biometric information without the user's permission or knowledge, or gathering biometric data without explicitly defined purposes
- Unauthorized use – using biometric information for purposes other than those for which it was originally acquired
- Unauthorized disclosure – sharing or transmitting biometric information without the user's explicit permission
- Unique identifier – using biometric information to track a user across various databases, to link different identities, and to amalgamate personal data for the purposes of surveillance or social control

DATA PROTECTION OFFICE

- Improper storage – storing biometric information in logical proximity to personal data such as name, address, social security number
- Improper transmission – transmitting biometric information in logical proximity to personal data such as name, address, social security number
- Forensic usage – using biometric information to facilitate investigative searches, which may be categorized as unreasonable search and seizure
- Function creep – gradually using biometric data for a variety of purposes beyond its original intention and scope

DATA PROTECTION OFFICE

IS BIOMETRIC DATA SENSITIVE INFORMATION?

- Biometric information is itself sensitive information. It is a unique, high quality data about a person's physical characteristics which needs to be treated with care. When we collect biometric information from a person, we are not just collecting information **about** that person, but information **of** that person. Biometric information cuts across both informational privacy and physical privacy. It can reveal sensitive information about us; our health, genetic background, age and it is **unique** to each of us.

DATA PROTECTION OFFICE

- Because biometric data is sensitive, and there are situations in which biometric systems could be misused, protections tantamount to the deployment-specific risks are necessary at all possible stages of the data's lifecycle.

DATA PROTECTION OFFICE

DO BIOMETRIC COMPARISONS RESULT IN EXACT, 100% MATCHES?

- Unique biometric templates are generated every time a user interacts with a biometric system. As an example, two immediately successive placements of a finger on a biometric device generate entirely different templates. and never generate an identical template.
- Therefore, for most technologies, there is simply no such thing as a 100% match. This is not to imply that the systems are not secure .

DATA PROTECTION OFFICE

IS THE DPA TECHNOLOGICAL NEUTRAL AND WHY?

- DPA is technologically neutral meaning that it regulates information handling without referring to specific technologies that facilitate information handling.
- Technological neutrality does not mean that we should not take into consideration technological change.
- Technological neutrality allows the DPA to be adequately flexible to accommodate technological change.
- A privacy regime must not go out of date every time technology changes!

DATA PROTECTION OFFICE

- Biometrics technology is a science , the ambit of which has not yet been clearly defined. There are many aspects of that technology which have not yet been discovered in their entirety.
- Is it then wise to say that they are 100% reliable?
- Obviously not. This is why we need some very strong safeguards, both in terms of physical and technical security safeguards to be able to defeat any potential side effects this technology may have on the privacy rights of individuals, if we opt to use it in our daily lives, coupled with effective laws such as the Data Protection Act.

DATA PROTECTION OFFICE

THANK YOU

ANY QUESTIONS OR COMMENTS?