澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
個人資料保護辦公室
Gabinete para a Protecção de Dados Pessoais

Unofficial Translation

On using attendance devices of biometric technologies other than fingerprint or hand-geometry identification

Questions:

(1) Given the consent of their employees, can an employer institution use attendance device of any currently available biometrics technology for the purpose of verifying employee identity and attendance, in compliance with the law governing personal data collection and processing?

(2) If hand-geometry, iris, vocal and facial features all fall in the category of biometrics technology, why is it that your guide designates hand-geometry verification as the tool for general attendance purposes? From the perspective of IT technology, almost all biometric identification technologies rely on digitising image data derived from a reader, and abstracting their characteristics by computation. Since iris, vocal and facial data play the same function as that of hand-geometry, how can using iris, vocal or facial identification technologies enhance security in any way?

(3) If at the time of promulgation, the law had been made based on devices available then that could only read hand-geometry data, would now be the time for the law to be updated with the current state of technologies? Can employers legally use any biometric identification devices currently available for attendance purposes?

Answer:

1. In reply to the many enquires received about whether an employer institution may, for attendance control purposes, use finger-prints or hand-geometry attendance devices, this Office has, exercising the power of the public authority referred in Law No. 8/2005 (the *Personal Data Protection Act*) and in No. 3 of Article 79 of the Civil Code, prepared and made available to the public a regulatory guide on using fingerprint /hand-geometry attendance devices.

2. The fingerprint /hand-geometry devices referred to here are those that use biometrics technologies for employee verification in attendance control processes.

3. One should note that this Office points out in the guide that where employers use

fingerprint /hand-geometry devices for employee attendance control, they must comply with the provisions of the *Personal Data Protection Act.* They must observe the principle of good faith, of proportionality, of respecting personal data privacy, of avoiding data processing for purposes other than that of data collection, of keeping personal data not longer than necessary. They must meet the criteria of legitimacy in data processing as provided in Article 6, and the rights of the data subject as provided for in Article 10-12, as well as observe the guidelines provided by this Office (including, in particular, that where it is impractical or where technical precautionary measures are inadequate, avoid using such biometrics verification equipment as fingerprint /hand-geometry devices for attendance purposes). In other words, using fingerprint /hand-geometry devices must be subject to certain restrictions.

4. Technically, there are other biometric identification technologies available apart from fingerprint /hand-geometry devices, such as those based on facial, vocal and iris data. Here, drawing on specialist observations, we offer an analytical table of the various biometric identification technologies in terms of their principles, characteristics, scope of data collection, mode of data collection, as well as their advantages and deficiencies, for people's reference:

Biometric identification technologies	**Working principles**	**Advantages**	**Disadvantages**	**Active/Passive data sampling**[1]
Fingerprint /hand-geometry device	Finger-prints, palm geometry or ultra-red light image data are collected in advance, which are then converted to a digital form that is compatible with and stored on a particular device.	Fingerprints and body structure do not change with time or personal emotions.	Body skin may become coarse, worn out with aging and thus adversely affect the reading efficiency.	Active

[1] In general, biometric identification falls in two categories – active and passive. In active sampling, the user initiates the operation of the biometric device, while in the passive mode the user does not need to go through the prior data sampling procedure before using the device.

Facial identification device	These usually make use of facial features such as iris, nose, corner of mouth, and turns their profiles, sizes, positions and inter-distances and angles to one another into mathematical patterns, and makes verification by comparison	The features do not change with time or personal emotions.	Verification accuracy and efficiency may be adversely affected by body posture angle, ambient light, hair, jewelries, aging, obesity, etc; such devices do not distinguish between twins.	It may be used passively
Vocal identification device	Identity verification is achieved by vocal spectrogram comparison.	---------	The technology is susceptible to influence by ambient noise, physical or emotional status; with problematic accuracy; susceptible to cheating with pre-recorded voice and imitation	It may be used passively
Iris identification device	The human iris covers unique lens, and contains fine stripes, dots, dentures, radius, wrinkles and streaks, etc. The device takes pictures of the iris and uses them to make identification and verification.	Data do not lend to easy duplication and forgery, and as such is safer as an approach.	When taking data samples, the device shines a beam of low-charge light on the eye of the user, which may cause fear and psychological resistance; High device cost.	Active

5. From the above table it is obvious that each identification technology has its own principle and characteristics:

(1) Active or Passive data sampling

Fingerprint /hand-geometry and iris identification devices are of the active data sampling type, which require the user to undergo a data sampling process before using the device. Therefore, the resulting data samples are more accurate compared with that obtained with passive data sampling devices, with less susceptibility to ambient influence. In contrast, facial and vocal identifications may be used with passive sampling devices, which do not require the user to undergo a prior sampling procedure. Such devices generally take a person's data samples through a camera or microphone and instantly perform data identification. In such a process of data sampling, the user may not be aware or told that their data are being collected. Therefore, the data collecting approach adopted by such devices is intruding. Passive or intruding data sampling devices have a potentially greater impact on the privacy of the people involved. Moreover, biometrics data collected this way may lend to abuse that is unknown to the data subject, or even used for secret surveillance. If attendance control is the only intended purpose, using such devices and data risks breaching the principle of reasonability.

(2) How the technologies affect the users

All biometric identification devices have an impact on the user in one way or another. For example, in its data sampling process, an iris identification device shines a beam of low-charge light on the eye of the user, which may cause fear or psychological disturbance; facial identification devices, on the other hand, may take longer in getting the data because of its susceptibility to influence from ambient light, the presence of hair or ornaments. It suffers a relatively higher error rate. The data such devices yield tend to be indicative of a person's gender and race, which may be sensitive data and therefore it may give rise to dispute. Vocal identification devices need the user to utter a certain sound in order for data sampling to complete, which may leave the user a feeling of being forced or manipulated. In comparison, fingerprint /hand-geometry devices are less intruding in data collection.

(3) Technical maturity

Fingerprint identification came earlier than most other biometrics technologies, and is relatively mature, with high accuracy of data sampling.

(4) Degree of popularity and acceptance

It is well known that fingerprint technology has been used widely in personal identity verification for its low cost, efficiency of identification, and ease of use. It is relatively popular in Macao. It gains popularity probably because Macao's personal identity laws have long required citizens to have their fingerprints and palm prints registered. Therefore, fingerprints and palm prints as biometrics data for identity verification are widely accustomed to, with a relatively high degree of acceptance.

(5) Scope of use

Generally speaking, people tend to use fingerprint /hand-geometry identification devices where attendance control is the only purpose of data collection. Under special circumstances, however, as in a healthcare institution, people tend to adopt devices that use technologies other than fingerprint /hand-geometry in order to avoid health hazards. Biometric identification technologies other than hand-geometry are mostly used for other purposes such as gate keeping where security is a concern, as well as to avoid over-collection and over-use of personal data.

6. In view of the fact that fingerprint /hand-geometry identification as a technology is relatively mature, and is popularly used, with better data sampling accuracy and less impact on the user, this Office advise that, where attendance control is the only intended purpose, employers should limit their use of biometrics technology to that of hand-geometry (including palm shapes, infrared-ray palm images, etc.); where there is no particular needs, attendance devices using facial, vocal and iris data should be avoided.

7. Of course, this does not mean that employers may not use devices of other biometrics technologies for attendance control; it only means that in utilising other technologies employers must heed the provisions of the *Personal Data Protection Act*, as well as this Office's specifications in this regard, and must have good reasons. This Office will conduct further research into attendance devices that use biometrics technologies in response to societal needs, and will prepare and publish relevant regulatory guides for people's reference.

(Updated on 7 September 2009)