Hong Kong General Chamber of Commerce
Roundtable Luncheon
13 April 2016

Collection and Use of Biometric Data

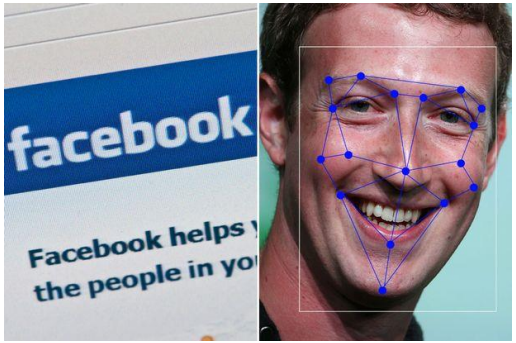
Stephen Kai-yi Wong
Privacy Commissioner for Personal Data, Hong Kong


Nowadays, leaving a digital footprint is inevitable

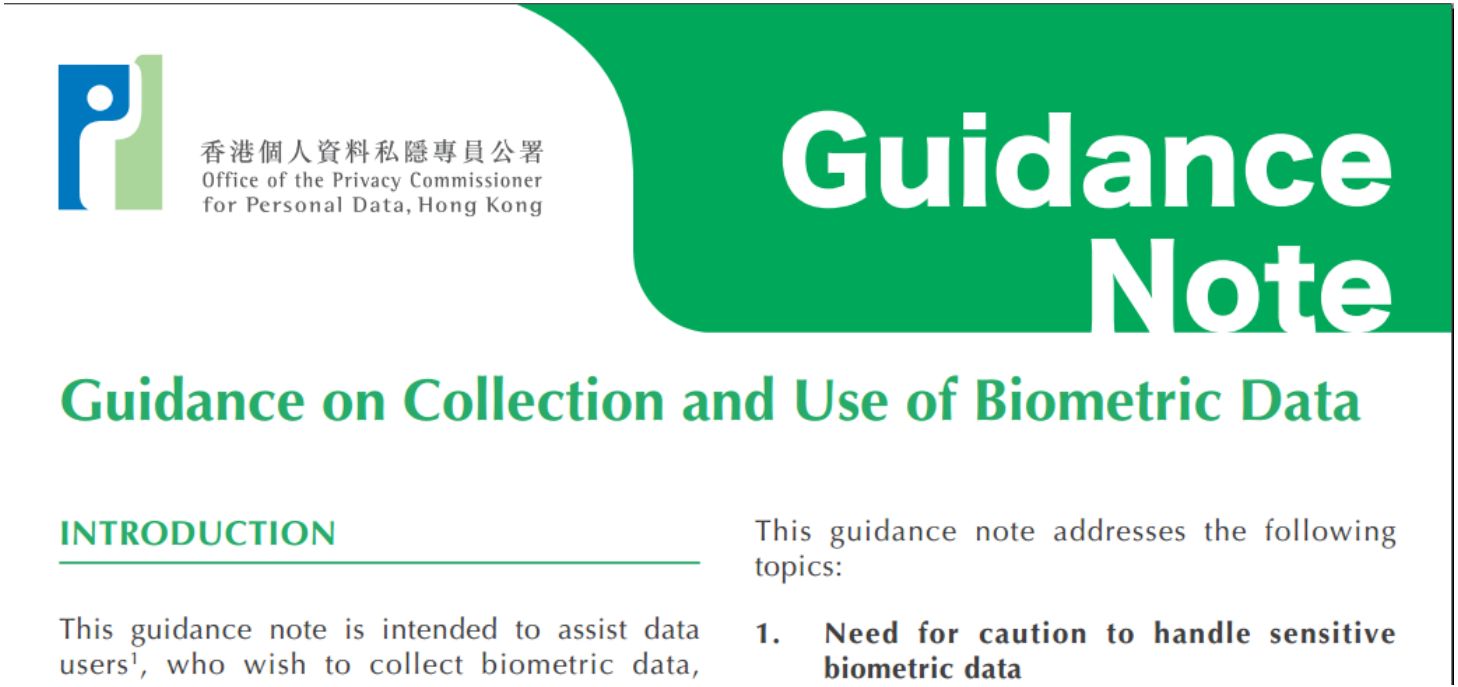
Biometric Applications

Everyday biometric applications:

- facial recognition in social media
- fingerprint door locks



Guidance on Collection and Use of Biometric Data



香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Guidance Note

Guidance on Collection and Use of Biometric Data

INTRODUCTION

This guidance note is intended to assist data users[1], who wish to collect biometric data,

This guidance note addresses the following topics:

1. **Need for caution to handle sensitive biometric data**

Collection and Use of Biometric Data

1. The Personal Data (Privacy) Ordinance
2. Biometric data and personal data
3. Characteristics and risks of biometric data
4. Justification in collecting biometric data
5. Risk minimisation techniques
6. Free and informed choice
7. Privacy Impact Assessment
8. Practical measures
9. Case sharing and overseas developments

What is Personal Data

Personal Data should satisfy three conditions:

- **relating directly or indirectly to a living individual**
- **from which it is practicable for the identity of the individual to be directly or indirectly ascertained**
- **in a form in which "access to" or "processing of" the data is practicable**

How Personal Data (Privacy) Ordinance Protect Customers

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性儲存及保留 Accuracy & Retention

資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達致原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

Principle 1 – Purpose and Manner of Collection

- related to the functions or activities of the data user
- lawful and fair means
- adequate but not excessive

Principle 1 – Purpose and Manner of Collection

Data subject be informed of:

- purposes of data collection
- classes of persons to whom the data may be transferred
- whether it is obligatory or voluntary for the data subject to provide the data
- where it is obligatory for the data subject to provide the data, the consequences for him if he fails to provide the data
- name or job title and address to which access and correction requests of personal data may be made

Principle 2 – Accuracy and Duration of Retention

Data users to take practicable steps to ensure:

- **accuracy of personal data held by them**
- **personal data not being kept longer than is necessary for the purpose**
- **when engaging a data processor to process personal data, contractual or other means being adopted to prevent any personal data transferred to the data processor from being kept longer than necessary**

Principle 3 – Use of Personal Data

- not being used for a new purpose without prescribed consent

"new purpose" - any purpose other than the purposes for which they were collected or directly related purposes

Principle 4 – Security of Personal Data

- practicable steps being taken to ensure no unauthorized or accidental access, processing, erasure, loss, use and transfer

Principle 5 – Openness – Information be Generally Available

Data users to provide:

- policies and practices in relation to personal data
- kinds of personal data held
- main purposes for which personal data are used

Principle 6 – Access to Personal Data

Data subject be entitled to request:

- access to his personal data
- correction of his personal data

What is Biometric Data?

Physiological data born with an individual

- DNA samples, fingerprint, palm veins, iris, retina
- facial images and hand geometries

Behavioural data developed by an individual

- hand writing pattern, typing rhythm, gait, voice

Is Biometric Data Personal Data?

Totality test:

- **biometric data alone (e.g. fingerprint) may not reveal identities**
- **biometric data in a database that links customers/staff members is personal data**

Is Biometric Template Personal Data?

Biometric data is not stored, only its representation

- **representation (called a template) is encrypted and stored as a meaningless number, and is not personal data**
- **if an organisation can decrypt the number and links it to an individual, it is personal data**

Fingerprint Image Cannot be Reconstructed?

IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 9, SEPTEMBER 2007 1489

Fingerprint Image Reconstruction from Standard Templates

Raffaele Cappelli, Alessandra Lumini, Dari

Abstract—A minutiae-based template is a very compa

Fig. 18. From left to right: an original fingerprint, a reconstructed fingerprint from the corresponding ISO template, and an overlay of the two images.

Is Biometric Data Personal Data?

Purpose test:

- **does it belong to an individual?**
- **does it identify an individual?**
- **if both are ‘Yes’, then biometric data is personal data**

Is Biometric Data Trustworthy?

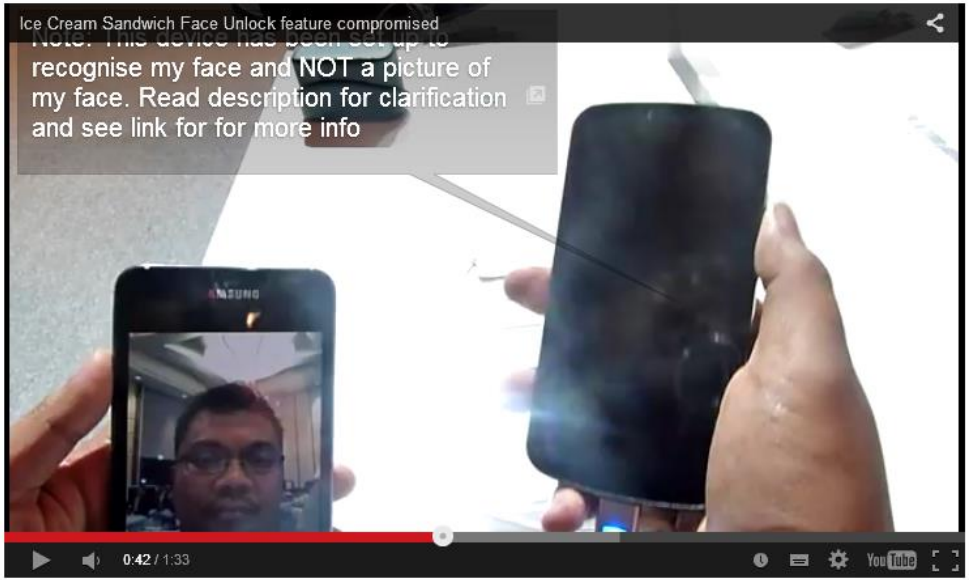
- biometric data is often unique and therefore trustworthy
- biometric recognition systems may not be so

Is Biometric System Trustworthy?

- Simple fingerprint recognition system can be fooled by ‘fake’ fingers

Is Biometric System Trustworthy?

- Android's facial recognition screen lock can be bypassed by a photo



Why Does Biometric Data Need to be Protected?

Permanency:

- once leaked, forever leaked – unlike passwords - one cannot change his fingerprints or DNA after leakage
- implication - lead to identification, impersonation, identity theft, misuse…

Why Does Biometric Data Need to be Protected?

Inference:

- DNA, retina, vein pattern may reveal the ethnic, and health and mental condition of individuals
- implication – discrimination in selection process such as employment, offering of insurance, etc.

How Can Risk of Biometric Data be Assessed?

Uniqueness/Changeability: The more unique, the more certain of the identity

- hand writing
- gait
- hand geometry
- face
- DNA
- fingerprint

How Can Risk of Biometric Data be Assessed?

Multipurpose: If the biometric data can be used for more than just identification

- face (race)
- fingerprint (criminal record)
- palm vein (physical health conditions)
- retina (physical health conditions)
- DNA (physical and mental health conditions, probability of diseases)

How Can Risk of Biometric Data be Assessed?

Covert collection: Can the biometric be collected without the knowledge of the individual?

- face (pinhole camera, sideway facial recognition)
- iris (can be captured easily with high resolution cameras)
- DNA (covert collection is not too difficult)
- fingerprint (normally require putting finger on scanner)
- retina (require direct staring)

Impact on Individuals

Risk factors	DNA	Fingerprint	Facial images	Handwriting pattern	Hand geometry
Uniqueness	High	High	Medium	Low	Low
Likely change with time or deliberately	No	No	Child/adult	Yes	Yes
Multiple purposes	Yes	Yes	Yes	No	No
Covert collection	Yes	Depends	Yes	Unlikely	No
Impact on individuals	Grave	High	Some	Some	Small

Justification for Using Biometric Data

Justifications

- lawful purpose directly related to the organisation
- necessary and not excessive
- benefit outweighs the potential privacy intrusion
- the types of biometric data involved
- no less privacy intrusive alterative available

Justification for Using Biometric Data

Examples

- ✓ access to biohazardous laboratory using iris/retina scanner
  - facilities can only be accessed by qualified personnel for public health issue
  - hand-free access required

Justification for Using Biometric Data

Examples

- ✓ access to construction sites by qualified workers using hand geometry
  - health and safety requires only qualified workers on site
  - employment of illegal worker is a criminal offence
  - theft prevention
  - use of identity card or smartcard is not practicable

Justification for Using Biometric Data

Examples

- recording attendance by fingerprint to avoid buddy-punching
  - buddy-punching was discovered by existing CCTV monitoring
  - penalty/monitoring mechanism needs improving, not changing to biometric system
  - no genuine consent was obtained

Justification for Using Biometric Data

Examples

- library and lunch-box management in schools
  - convenience is no excuse for privacy intrusion
  - minors are not in a position to understand the implications

Risk Minimisation Techniques

Administrative measures

- collect as few details, and from as few people, as possible
- use only in necessary places
- distinguish between
  - identification
    - the system compares everyone in the database until a match
  - authentication
    - one declare who he is, the system matches one specific record in database

Risk Minimisation Techniques

Technical measures – Use of smartcard to store template

- how it works:
  - template stored and encrypted in smartcard, to be kept by the individual
  - individual presents card to scanner to read template
  - individual has biometric data scanned
  - if the two match, the identity of the individual is authenticated

Risk Minimisation Techniques

Technical measures – Use of smartcard to store template

- decentralised so data breach will be less serious
- organisation normally has no access to template so less chance of misuse
- template encrypted in smartcard which contains no other personal data so risk of card loss is small
- a form of authentication so fewer biometric details needed

Free and Informed Choice

Individuals should be provided with free and informed choice to use biometric data

- transparent notice on the purpose, obligation, transferal and possible adverse action
- not under undue influence (employer-employee, school-pupil)
- genuine alternative offered
- data subject has the mental capacity to understand

Privacy Impact Assessment

PIA – a systematic process to evaluate a proposal in terms of personal data privacy impact

- the need for biometric data collection
  - a) genuine necessity; b) problem be fixed without biometric data?
- whose biometric data should and could be collected
  - a) limit number and duration of collection; b) genuine choice offered?
- the extent of biometric data to be collected
  - a) identification vs authentication; b) complete image not necessary

Practical Measures

1. Strong control over data access, use and transfer

- have clear policy in place to govern data access, use and transfer
- avoid function creep
- ‘need-to-know’ basis

Practical Measures

2. Retention of data

- personal data not kept longer than necessary (legal requirement)
- regular purge when no longer needed
- retention policy
- may be anonymised instead of erased

Practical Measures

3. Accuracy of data

- a legal requirement
- if adverse action may be taken based on biometric data, accuracy is even more important
- accuracy and limits of biometric recognition system must be known
- if adverse action is to be taken, individual must be offered opportunity to redress

Practical Measures

4. Secondary use

- consent required for the change of use (legal requirement)
- some biometric data carry other information about individuals (such as health conditions and potential health conditions), any secondary use must have consent from individual

Practical Measures

5. Security

- reasonably practicable measures to ensure protection (legal requirement)
- expectation on such measures is high as the harm of data leakage is potentially grave
- general advice – encryption during storage and transmission, access control for those need-to-know, and regular review

Practical Measures

6. Privacy policy availability

- Privacy policy being made available (legal requirement)
- clear policy for staff, contractor and customer concerning:
  - rules of collection, holding, processing and use of biometric data
  - data access and correction procedures
- review mechanism in place to ensure effectiveness

Practical Measures

7. Staff training

- training, guidance and supervision to be given to staff members
- new staff members are trained as soon as possible
- refresher for existing staff members

Practical Measures

8. Use of contractors

- contractual or other measures in place for retention, misuse and security for contractors (legal requirement)
- personal data processing may be outsourced but legal liability remains

Local Example

Fashion trading company fingerprint system on staff attendance and security

- collection and use of fingerprint must be justified
- theft were caught by CCTV cameras in the past
- sufficient security measures, including locks and CCTVs, were in place
- company only has 20 staff, attendance can be monitored effectively by other measures
- employees were not given choice
- company found to have collected excessive personal data unfairly

Overseas Case - Canada

Canadian Privacy Commissioner found LSAC contravention

- fingerprints were by the Law School Admission Council for enrolment to its tests
- LSAC could not produce evidence of frauds in the past
- collected fingerprints were never needed for verification
- Canadian Privacy Commissioner concluded the privacy intrusiveness was greater than the potential benefit
- LSAC changed to collect photos instead

Overseas Developments

Australia – biometric data = sensitive personal data and can only be collected with consent

EU – General Data Protection Regulation also included biometric as sensitive personal data

Canada – guidance on Data at your fingertip

Ireland – guidance on Biometrics in the workplace

UK – guidance on Biometric system for schools


danke
謝謝
ngiyabonga
teşekkür ederim
спасибо
dank je
thank you
gracias
tapadh leat
bedankt
hvala
mauruuru
mochchakkeram
dziękuję
go raibh maith agat
sukriya
kop khun krap
sagolun
obrigado
arigatō
takk
dakujem
grazie
terima kasih
мерси
감사합니다
merci
ευχαριστώ