



中國醫學科學院

Chinese Academy of Medical Sciences

中國協和醫科大學

Peking Union Medical College



The *Status Quo* and Ethical Governance in Biometric in Mainland China

**Third International Conference on Ethics and Policy
Biometrics and International Data Sharing
4-5 January 2010, Hong Kong**

ZHAI Xiaomei Ph.D

Centre for Bioethics

Chinese Academy of Medical Sciences

Peking Union Medical College

Disclaimer

- **The opinions expressed in this presentation are my own, They do not reflect any position or policy of CAMS or the National Ethical Committee of MOH that I serve for.**

My presentation is preliminary. So the aim is to "Throw out a brick to attract a jade" (抛砖引玉).

General Outline

- **Introduction**
- **Status quo of biometrics in mainland China**
- **Ethical concerns**
- **Ethical governance**

Introduction

"Blade Runners" 刀锋战士

In 1982 an American science fiction film "Blade Runners" depicts a story in November 2019 Los Angeles in which genetically engineered beings called

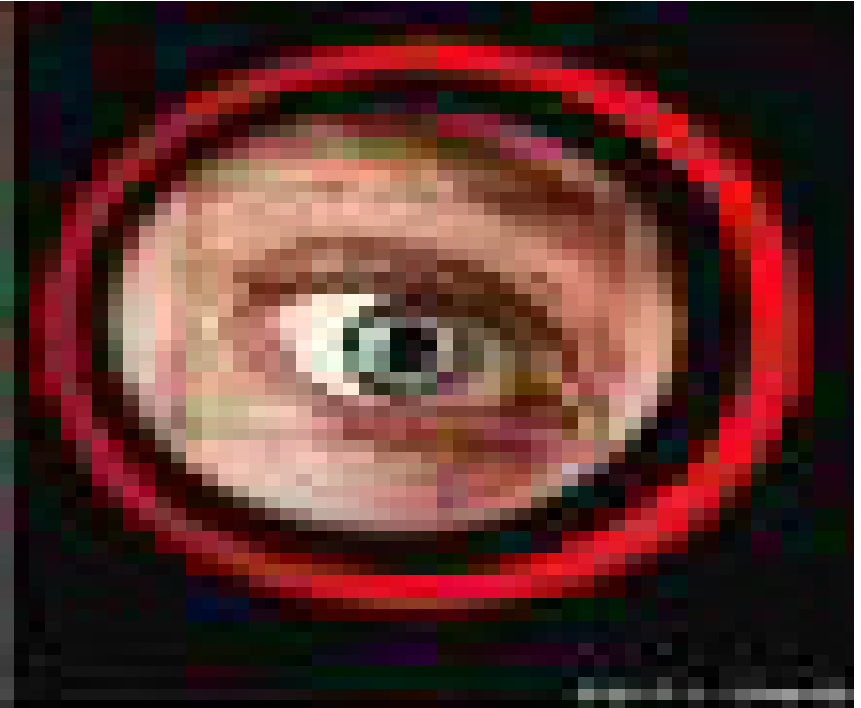
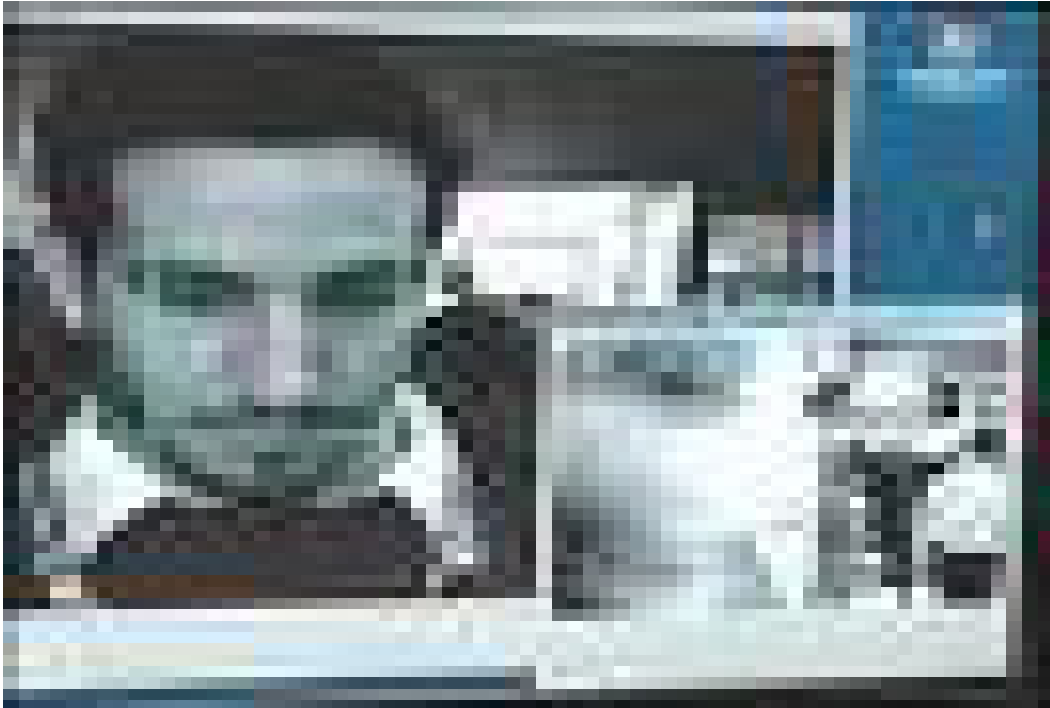
Replicants (visually indistinguishable from adult humans) are manufactured by the all-powerful Tyrell Corporation.



"Blade Runners" 刀锋战士

As a result of a violent Replicants uprising, their use on Earth is banned, and Replicants are exclusively used for dangerous or unskilled work as slaves in Earth's colonies. Any Replicant who defies the ban and returns to Earth is hunted down by police assassins known as "blade runners". Replicants can be identified only by using a machine, which analyzes the iris contractions and dilatations. The machine that allows to identify the Replicants, actually, is a biometric device.

No longer a science fiction, biometric technologies are the most important innovation in the IT industry for the coming years and the biometric industry is projected to grow up greatly.



Definition of Biometric Technologies

- **Biometric technologies can be defined as automated methods of recognizing or verifying the identity of a living person based on a physiological or behavioural characteristic.**
- **Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In IT biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.**

Two Classes of Biometric Characteristics

- **Physiological are related to the shape of the body.**
Examples include, but are not limited to fingerprint, face recognition, DNA, hand and palm geometry, iris recognition, which has largely replaced retina, and odor/scent.
- **Behavioral are related to the behavior of a person.**
Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term **behaviometrics** for this class of biometrics.

Parameters for Human Characteristic Being Used for Biometrics

- **Universality** – each person should have the characteristic.
- **Uniqueness** – is how well the biometric separates individuals from another.
- **Permanence** – measures how well a biometric resists aging and other variance over time.
- **Collectability** – ease of acquisition for measurement.
- **Performance** – accuracy, speed, and robustness of technology used.
- **Acceptability** – degree of approval of a technology.
- **Circumvention** – ease of use of a substitute.

Two Modes of Operating by a Biometric System

- **Verification** – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number.
- **Identification** – A one to many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual.

Applications of Biometric Technologies

- **Applications of the technology include checking the identity of passengers at borders, checking the identity of entrants at the gate of public events, proving the identity of payments, social security, and others benefits claimants, restricting access to secure premises, checking the identity of voters at polling booths and identifying known criminals,.**

Advantages of Biometric Technologies

- **More accurate**
- **More reliable**
- **More effective**
- **More confidential**
- **More convenient**
- **Would be cheaper: For example, a fingerprint scanner that cost \$3,000 five years ago, with software included, and \$500 two years ago, costs \$100 today.**

Status quo of Biometrics in China

Past and Present

- **The use of fingerprints in commercial and judicial practices has thousands of years history.**
- **Starting in 1990s there are 6 major centres for biometric R and D under the support of 863 and 973 focus programmes which funded by the Ministry of Science and Technology of China.**

Leading R&D Teams in China

- **Biometric Research Center, Hong Kong Polytechnic University**
- **Center for Biometrics and Security Research (CBSR) Institute of Automation, Chinese Academy of Sciences (CASIA)**
- **Joint R & D Laboratory for Advanced Computer and Communication Technologies (JDL), Institute of Computing Technology, Chinese Academy of Sciences (CASICT)**
- **Electric Engineering Dept, Tsinghua University**
- **Center for Information Research, Peking University**
- **Center of Forensic Sciences, Beijing Genomics Institute**

Technologies Developed

- **Face (Visible Light & Near Infrared)**
 - CASIA
 - Institute of Computing Tech, CAS
 - Tsinghua University
- **Fingerprint**
 - CASIA
 - Peking University
 - Many Companies
- **Iris**
 - CASIA
- **Palmprint**
 - Hong Kong Polytech Univ
 - CASIA

Application in Olympic Game

- **At opening & closing ceremony of 2008 Beijing Olympic Game 100, 000 audience passed 100 gates by speedy identity verification with facial recognition systems.**
(Individual information and a photo were required to provide when audience bought the ticket).

Application in Shenzhen Customs

- **There are 600,000 passengers who exit from or enter into Shenzhen customs per day.**
- **After using facial recognition devices, the time of customs checking per passenger is reduced from 13 seconds to 6 seconds.**

Application in Training Management

- **For improving the quality of training for novices and prevent fraud and "street killers", an intelligent driving training management system (biometric device) has been used in Suzhou City since 2008.**

Significant Biometric Applications

- **Governmental**
 - **Self-Service Border-crossing (deployed)**
 - Shenzhen – Hong Kong Boarder since June 2005
 - Zhuhai – Macau Boarder since April 2006
 - **Biometric E-Passport (on-going)**
- **Enterprise: Time attendance and access control**
 - Finger, Face, Iris, Palm**
- **Consumer products**
 - Face Logon – on notebook PC**
 - Finger Logon – on mobile phone, PC**
 - Finger Lock**

Demands Increasing

- **Demands from**
 - **social security:** finger and facial recognition may prevent false claims for pensions(养老金) and subsistence allowances (低保金) (Ministry of Social Securities).
 - **public security:** among 250 millions output values of biometric products more than 40% are used in public security and police.
 - **finance departments:** prevent fraud and false claims in finance. And,
- **If the government decides to use biometric identification cards and passports, it would be a huge demand.**

Future Prospect

- **There are near 200 enterprises which join the R&D and marketing of biometric products, and the output values in market is near CNY 300 millions *yuan*.**
- **China would be great market for biometric products and important provider of biometric technologies as well.**

Challenges

- **no national standards for biometric products and applications**
- **almost no public discussion on ethics, policy and governance issues of the application.**
- **lack of privacy law, traditionally lack of the privacy awareness:**

If you have something that you don't want the other people to know, you should not do it in the first place.

---Natasa Pire Musar

若要人不知,除非己莫为.----中国格言(Chinese proverb)

Case of “Data Gate”

- **In 2008 the hot topic was the case of Amorous Photo (Amorous Photo Gate 艳照门).**
- **In 2009 the case of Data Gate (资料门) became the most concern in mainland China according to CCTV news reported on 2 January;**
- **One Network Advertising Company in mainland claim to provide a free trial software on the computer of property management office for facilitating communication between this office and owners. The all owners' detailed personal data was transferred to the company's server with in one minute when they install this software;**

Case of “Data Gate”

- **Shenzhen branch of the company collected these data and its Beijing branch sold it. It led to serious harassments, blackmails and even crimes.**
- **There are also black data market in China. At internet some claim they have 65,000 stockholders data could be sold with the price 3000 yuan, about 40,000 bosses' mobile number could be sold with 200 yuan. and detailed data of 600,000 car owners in Guangzhou could be sold with less than 2000 yuan.**
- **All kind of personal data could be sold! Privacy protection has emerged as a grave issue of public concern.**

Ethical Concerns

Privacy

- **Physical or mental characteristics or conditions might be deducible from biometric measurements.**
- **The most significant privacy concerns raised by biometrics relate to the threat of “function creep”, by which the original purpose for obtaining the information is widened to include the purposes without the informed and voluntary consent of the participants.**

Stigmatization and Discrimination

- **Recent scientific research suggests that biometric features can *per se* disclose medical information. Certain chromosomal disorders – such as Down’s syndrome, are known to be associated with characteristic fingerprint patterns in a person.**
- **Thus, biometrics might become not only an identifier, but also a source of information about an individual.**
- **And future and likely use of genetic test information and DNA profiles in biometrics bear many risks of discrimination and the multiplication of compulsory testing procedures.**

Stigmatization and Discrimination

- **Various groups, including the elderly and disabled faces the risk of discrimination.**
- **Fingerprints become less readable with age, while those who are visually impaired or have a limb missing may not be able to provide the requisite biometric data; and severe pain and serious injuries may prevent some patients in emergency wards from providing biometric characteristics.**

Dangers to Owners of Secured Items

- **When thieves cannot get access to secure properties, there is a chance that the thieves will assault the property owner to gain access.**
- **If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Benz owner when attempting to steal the car.**

Lose Identity

- **Some worry that today's citizens will become biological data, as name, age, address and other traditional identifying characteristics are replaced by biometrics which could be used by companies and governments alike.**
- **On the other hand, many people in developing countries do not possess any documents with which they can prove who they are. These people are already vulnerable on account of their poverty, and the fact that they are unable to provide evidence of their identity makes it difficult to empower them.**

Unease & Worry (1)

- **Taking the fingerprints of staff is not likely to improve morale - they might feel their superior is looking over their shoulders - and the associations with criminality worry a surprising number of people.**
- **A huge database containing this sort of personal information would unnerve staff. If such a system were to be compromised, the results could be devastating.**
- **Worry on the possibility of infectious diseases to be transmitted via fingerprint-scanner devices.**

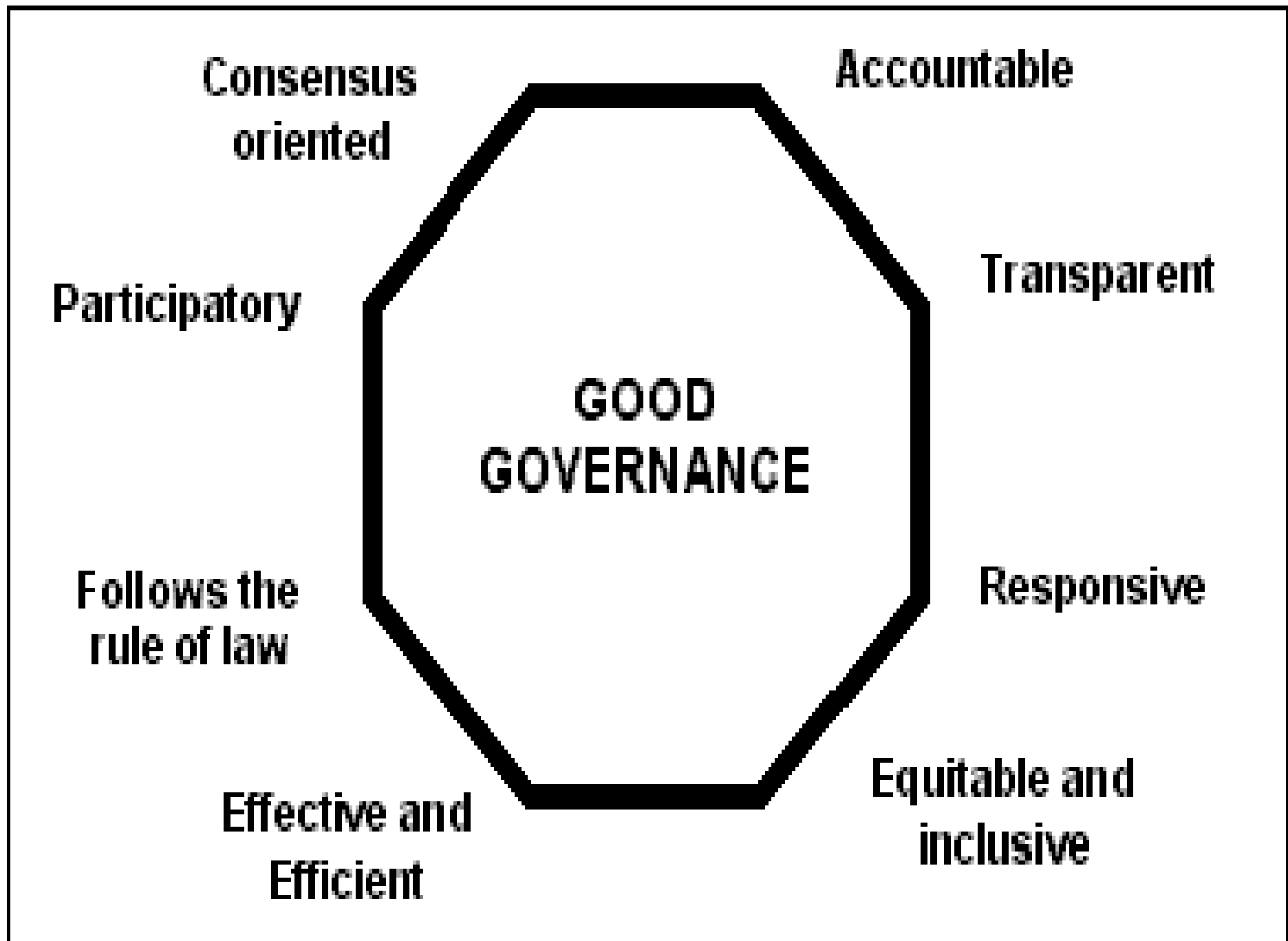
Unease & Worry (2)

- **One advantage of passwords over biometrics is that they can be re-issued. If a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it.**
- **There are ways to cheat the technology. Artificial devices could be used for mimicry, and the reliability of data is dependent upon the source that provided it. Biometric identification could be fooled by a latex finger, a prosthetic eye, a plaster hand, or a DAT (digital audio tape) voice recording.**

Public Concerns

- **Furthermore, public concerns about the use of biometric technologies may focus on:**
 - **The pervasiveness of a technology which many people do not understand.**
 - **The lack of transparency of the work of biometric technologies and its effects on individuals and society.**
 - **The difficulty of respecting privacy and confidentiality when third parties may have a strong interest in getting access to biometrically recorded and stored personal data.**
 - **The difficulty in ensuring the security of shared personal data.**
 - **The lack of adequate infrastructure which may reinforce existing inequalities.**

Ethical Governance



Ethical Governance (BIONET)

European Commission F6

The concept of ethical governance arises from our understandings of the ways in which a governance system can be made both practical and just, in diverse historical, cultural and normative contexts. The following aspects define ethical governance in particular:

- Rule of law**
- Transparency**
- Accountability**
- Respect for human rights**
- Public engagement, and so on**

What do We Need?

- **We need an ethical framework for evaluating any conduct which will be taken in biometrics R&D and its application.**
- **This framework will be formed by a set of principles of ethical governance, the set of principles is also core values shared and committed by stakeholders who engage in biometrics R&D and its application.**

Principle 1

- **Fundamental purpose** of biometric R&D and its application is to promote well-beings and quality of life of people with safer, more effective, and more advanced science/technology (以人为本 take people as the foremost) .
- **Biometric technologies should be used solely for legal, ethical, and non-discriminatory purposes (International Biometric Industries Association, 1999).**
- **Any action in biometrics should be evaluated on the principles of beneficence and non-maleficence serving as a basis for the attempts to weigh anticipated benefits against foreseeable risks.**

Principle 2

- **Biometric R&D and its application should maintain high standards of **responsible** research, i.e. adhering research integrity and committing safeguarding and protecting people's rights and interests.**
- **“They are therefore committed to the highest standards of systems integrity and database security in order to deter identity theft, protect personal privacy, and ensure equal rights under the law in all biometric applications” (Mintie D, 1999).**

Principles 3

- **Conflict of interest between professionals, companies and users in biometric R&D and its application should properly be handled with. In any case people's (vulnerable in particular) well-being cannot be compromised for the interests of professionals or companies.**

Principles 4

- **Respect for persons, mainly **respect autonomy** serve as a basis for requirements of self-determination. The principle of informed consent must be adhered. In case of re-use of personal information for another purpose different from the purpose when enrolment, consent has to be sought.**

Principle 5

- **Human dignity serves as a basis for requirements of privacy, confidentiality and medical secrecy. It requires us not only to not infringe upon individual right of privacy/confidentiality, but also to do our best to prevent improper or illegal disclosures of private information.**

Principle 6

- **Justice serves as a basis for requirements of equitable distribution of limited resources, and prevention of possible stigmatization and discrimination due to improper disclosure of individual information.**

Principle 7

- **Solidarity** serves as a basis of the right for everyone to enjoy the benefits from biometrics R&D and application, **with a special concern for vulnerable groups in society.**

Principle 8

- **Transparency** requires biometrics R&D and its application should be made **transparent to the public**, i.e. taxpayers, and help them to know what is biometrics and what are the benefits and risks from its application.

Principle 9

- **Public engagement** requires us to take measures (such as the dialogue between biometrics professionals and the public or its representatives, NGO) to facilitate public understanding of biometrics and lead to public “consultation”, “engagement” or “involvement.” in the process of biometrics R&D and its application.

Good Governance (善治)?

There are three popular opinions in China for a good governance:

- 1. Develop (pollute) first, and govern second.(good governance?)**
- 2. Scientists only concern R&D, government and enterprises only concern investment, the public only concern enjoyment/consumption, and the humanists /social scientists only concern comments with hindsight(马后炮). (good governance?)**

Good Governance (善治)?

3. Governance should accompany development at initial stage and all stakeholders including government, scientists, engineers, humanists and social scientists, lawyers, businessmen, and the public need engagement in the governance from the very beginning. (good governance)

*Thank you very much
for your attention*