Privacy and Security Challenges in Deploying Biometrics in the EU

- A Data Protection Commission’s Perspective -

Biometrics Symposium 2008 - Tampa / Florida

Martin Meints
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein
ULD61@datenschutzzentrum.de
• Privacy vs. Data Protection

• Relevant data protection threats in the context of biometrics

• Data protection- and security-related recommendations for the application of biometrics in the EU

• Which aspects are relevant in contexts outside the EU? – A comparison with the Privacy Impact Assessment (PIA)

• (References)
Privacy research referring to biometrics shows an international exchange

- Ann Cavoukian (Can), Roger Clarke, Malcolm Crompton (Aus)
  - Privacy Impact Assessment (PIA, since 1998)
- Hes, Hooghiemstra, Borking (The Netherlands)
  - “At face value” (1999)
- International Biometrics Group (USA)
  - BioPrivacy Initiative (since 2000)
- Karen Curtis (Aus)
  - Biometrics Institute Privacy Code (since 2006)
- Ann Cavoukian (Can)
  - Biometric Encryption (2007)
Privacy vs. Data Protection

• Aspects of Privacy
  ▪ Information privacy
  ▪ Privacy of communication
  ▪ Bodily privacy
  ▪ Territorial privacy (The right to be let alone)

• Data Protection is dealing with personal data (data related to an identified or identifiable person)
  ▪ Legal grounds in the EU: European Directive 95/46/EC
  ▪ When applying a biometric system in an organization in European member countries, you can’t get around national Data Protection legislation
  ▪ Data Protection is related to information privacy and privacy of communication
Privacy vs. Data Protection

• In European member countries: Processing of personal data is prohibited unless proper legal grounds are in place
  - Does not or only partially apply for:
    - Systems for private use only
    - Application of biometrics in the context of state security
• Outside Europe (with a few exceptions): Processing of personal data is allowed unless prohibited by specific legislation

• Informational self-determination vs. data ownership

• Data Protection compliance check vs. Privacy Impact Assessment (PIA, mostly not mandatory)
Data Protection Principles and Biometrics

- Requirement of proper legal grounds
  - Law
  - Effective consent (informed, given explicitly)
- Purpose binding / Purpose limitation / Finality principle: Prevention of function creep
  - Data must be used for the purpose only for which they were originally collected
- Data minimization
  - Data not needed for the defined purpose are not to be stored & used; existing data have to be deleted as early as possible
- Proportionality
  - The amount and protection-worthiness of personal data needs to be proportionate for the purpose of data processing
Data Protection Principles and Biometrics

- Transparency and collection of data directly from the data subject
- Data subject’s rights
  - Access to own data, rectification, erasure
- Special categories of personal data are to be protected especially:
  - Racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, health-related data, and data concerning the sex life
- Technical and organizational security measures (state-of-the-art)
**General Data Protection Principles**  
*(not further covered here)*

- Organizational data protection requirements such as
  - data protection organization (e.g., a Data Protection Advisor or Officer),
  - data protection management (including internal and external audits, handling of data subjects requests, …),
  - prior checking,
  - reporting requirements,
  - special provisions for data processing in third countries (countries having a privacy protection regime below the level of the European Data Protection Directive)
  - etc.
Data Protection Risks related to Biometric Systems

- “Identity Theft”
- Function creep, e.g., by evaluation and use of additional information in reference data
- Linking of biometric data with other data sources, profiling
  - Anonymization of biometric reference data is not possible, or biometrics do not work anymore
- Tracking / surveillance / direct identification / “passive authentication”
  - Use of unobserved / unnoticed sensors, hidden matching, automated individual decision making
- Violation of informational self-determination by forcing data subjects to use biometric systems
- Unwarranted belief in technology though known fuzziness of decisions (FAR, FRR)
System’s Architecture

- Archive of reference data
  - Centralized
  - Decentralized
  - Who is in control of the reference data?
- Additional information in reference data (see following slides)
- Protection of reference data
  - Encryption?
  - Biometric encryption?
  - Other methods for template protection?
    - See, e.g., 2nd WD ISO/IEC 24725
System’s Architecture and Management Requirements

- How is the biometric system secured?
  - Two (or more) factor authentication for privileged accounts?
  - Anti-spoofing measures?
  - Open interfaces?
  - …
  - Information Security management system and concept taking the processing of special categories of personal data into consideration needed

- Reference to international standards is helpful, but not required:
  - CobiT 4.1
  - ISO/IEC 15408 (Common Criteria including Biometric Evaluation Methodology v1.0)
Fingerprinting

- Crossover
- Core
- Ridge Bifurcation
- Ridge Ending
- Island
- Delta
- Pore
Additional Information in Biometric Raw Data (Fingerprint Pictures)

- Dermal diseases
  - Eczema
- Worn papillary structures (caused, e.g., by hard labor)
- Nutrition state of the mother in the first three months of pregnancy
- Empirical studies give evidence that certain papillary structure are related with a certain likeliness with:
  - Racial origin
  - Geographic origin
  - To have or develop certain diseases, among them stomach problems
- Non-scientific neighborhood: palm reading
  - A “criminal’s thumb”


Data Protection Aspects of Antispoofing

- Typical approach: Liveness detection
- General Approach: Additional data are collected and evaluated:
  - Example: Conductibility of the skin on the finger tips
    - Depending on the context these data also may be used for “lie detection”
2D-Face Geometry
3D-Face Geometry (Elastic Bunch Graph)

Characteristics used are e.g.:
Geometry-related information
Color / texture of the face

...
Marfan Syndrome
Facial Palsy

Causes:
- stroke,
- inflammation of the nerve system

Peripheral facial palsy

Central facial palsy

When closing the eyes
A newly born baby ...
Cleft Lip
Additional Information in Biometric Raw Data (Face Geometry)

- **Diseases**
  - Liver diseases
    - Yellowish skin
  - Acne
  - Down Syndrome
- **And:**
  - Sex
  - Color of the eyes
  - Color of the hair
  - Ethnic origin
- **People are directly identifiable from their pictures**
Additional Information in Biometric Raw Data (Face Geometry)

- Methods for automated extraction of information from face pictures are already available.

- Despite the word spread by, e.g., the German Ministry of Interior, there is a big difference between a snapshot with a digital camera and the stored biometric raw data, e.g., used in the ePassport:
  - Why else are up to 10% of passport photos still rejected by passport authorities?
**MUSTERFOTO**

- Das Foto muss die Gesichtsebene der Person aus der Frontalrichtung zeigen. Die Gesichtsebene beträgt etwa 50-70% des Fotos. Das Gesicht von der Seite ist nicht zugelassen.
- Das Foto muss die Gesichtsebene der Person aus der Frontalrichtung zeigen. Die Gesichtsebene beträgt etwa 50-70% des Fotos. Das Gesicht von der Seite ist nicht zugelassen.
- Das Foto muss die Gesichtsebene der Person aus der Frontalrichtung zeigen. Die Gesichtsebene beträgt etwa 50-70% des Fotos. Das Gesicht von der Seite ist nicht zugelassen.

**FORMAT**


**SCHRÄGE UND KONTRAST**

- Das Gesicht muss in allen Bereichen scharf abgebildet, kontrastreich und klar sein.

**AUSLEUCHTUNG**

- Das Gesicht muss gleichmäßig ausgelichtet werden. Belichtungs- oder Schatteneffekte im Bereich der Augen sind zu vermeiden.

**Source:**

German Bundesdruckerei
Additional Information

- The highly standardized format of these photos also supports automated extraction of additional information and thus function creep.

- And: It can be expected that geometry-related health information (Marfan syndrome, facial palsy, cleft lip etc.) still may be present in templates if features used are geometry-related.
Handgeometry
Marfan-Syndrome

Disease mainly concerning Connective tissue
Gout and Arthritis
• Again: It can be expected that geometry related health information (gout, arthritis, marfan) still may be present in templates.
Iris-Scan
Additional Informationen in biometric raw data (isris scann - iritis)
Additional Informationen in biometric raw data (iris-scan)

- Results in Failure to Enrol:
  - Aniridia (missing iris)
  - Missing eyes
  - Pronounced Nystigmus (flickering of the eyelid)

- Again non-scientific neighborhood: Iridology
  - Based on a sectoral approach certain pattern of the iris are correlated with certain diseases or socio-psychological constitutions.
Additional Informationen in biometric raw Data (iris-scan)

• Liveness detection
  ▪ Standard method: reaction of the pupil on changing light conditions
    ▪ A reaction slowed down may indicate alcohol or drug consumption
Vein pattern
Additional Information in biometric raw Data (Vein scanning)

- Diseases:
  - High blood pressure
  - Varices
Genetic Fingerprinting

- Area of investigation:
  - Repeats of DNA-sequences in non-coding parts of the DNA (so called „Junk-DNA“), >95% of the overall DNA
Additional Information in biometric raw Data (genetic fingerprinting)

• DNA samples contain the complete genetic code

• Genetic fingerprint contain e.g.:
  ▪ Sex
  ▪ Relatedness
  ▪ Likeliness to belong to certain *ethnic or racial group*
  ▪ In one case (locus TH01) a certain allele indicates an increased likeliness to develop *type 1 diabetes*
Additional Information in Biometric Raw Data (Genetic Fingerprinting)

- Recent research indicates that junk DNA may be much more related to coding parts of the DNA than expected:
  - Rigoutsos, I., Huynh, T., Miranda, K., Tsirigos, A., McHardy, A., Platt, D., ‘Short blocks from the noncoding parts of the human genome have instances within nearly all known genes and relate to biological processes’, Proceedings of the National Academy of Science of the United States vol. 103 no. 17, pp. 6605-6610, Washington D. C., April 2006.

- Research question: Are non-coding parts of the DNA really non-coding?
Behavioural biometrics - Overview

- Diseases of the central nerve system such as Parkinson’s disease and stroke are included in the following biometric raw data:
  - Voice recognition
  - Hand writing
  - Key stroke dynamics
  - Gait analysis
Legal Aspects

• Applications of biometrics leading to automated individual decisions are prohibited

• In case biometrics are used based on effective consent:
  ▪ In working environment: consensus with the works council to use biometrics is needed
  ▪ A non-biometric backup procedure is needed
    ▪ Prohibition of coupling: the use of the biometric system must not be a requirement to use the service offered

• In cases of convenience-driven applications, data protection authorities decided that the use of centralized reference databases is not proportionate
  ▪ E.g., swimming bath in Mohnheim/Luxemburg
Recommendations

• Make sure that implementations of biometrics are built on proper legal grounds
• Don’t use biometric raw data as reference data
• Use methods to hamper linkage such as
  ▪ Decentralized storage of reference data
  ▪ Template protection methods, e.g., Biometric Encryption
  ▪ Distributed storage of biometric reference data and other personal data
• Consider revocable formats for reference data
Recommendations

- Check whether and how user control could be added, e.g., via use of:
  - Decentralized storage of reference data on token
  - Cryptography (key under control of the user)
  - Encapsulated biometrics
    - On-card sensors, matching and storage of reference data

- Keep properly to national data protection legislation
  - E.g., with respect to prior checking as special categories of personal data are processed
Privacy Impact Assessment (PIA)

- Frequently used in Australia, New Zealand, Canada, and USA based on standardized questionnaires
- Steps:
  - Project description
  - Mapping the information flow (focused on personal information)
  - Privacy impact analysis (core step)
  - Privacy management (investigate whether the procedures from a privacy point of view could be improved)
  - Recommendations
Core questions

- Compliance to privacy legislation?
- Do individuals have to give up control of information about themselves to any degree?
- Will it require, or is it likely to result in, individuals changing their behavior (e.g., having to present identification in more circumstances), or incurring costs?
- Will the project impact disproportionately on individuals or groups without identity documentation?
- Will decisions that have consequences for individuals be made on the basis of the personal information handled in the project (e.g., decisions about services or benefits)?
- Does the project deliver the right amount of accurate and relevant information to adequately inform these decisions?
- Is there provision for complaint-handling mechanisms, in the event that privacy breaches eventuate?
- Have emergency procedures been devised in the event that the system fails?
- Is there provision for audit and oversight mechanisms, including emergency procedures in the event that the system fails?
• Core questions
  ▪ Does the project include the potential for function creep (e.g., might there be an interest in using the personal information collected for the project, for other purposes) or other unplanned consequences?
  ▪ Assess the value of the information to unauthorized users (e.g., is it information that others would pay money or expend effort to gain access to)?
  ▪ Is any intrusion (physical or on property) or surveillance (whether covert or overt) fully justified and proportional to the outcome?
    ▪ Is it the only way of achieving the aims of the project?
    ▪ Is it done in the least intrusive manner?
    ▪ Is it subject to legislative or judicial authority?
  ▪ How consistent is the project with community values about privacy (e.g., does it involve new ways of identifying individuals, the creation of significant databases or the use of genetic material or information)?
  ▪ How has privacy been factored in the project's cost-benefit analysis, and the analysis of the project's return on investment?

Further Trends

• Data Protection Commissions in Europe increasingly get involved constructively in development and deployment of biometrics
  ▪ Involvement in international standardization (e.g. in the context of ISO/IEC working drafts concerning template protection and evaluation criteria for biometrics)
  ▪ Projects funded by the EC (e.g. TURBI NE)
With respect to technical and organizational security measures and privacy design, application of EU data protection legislation leads to similar results compared with PIA.

However, EU-specific, mainly organizational data protection measures have to be taken and privacy risks are considered differently.

In turn, EU-specific data protection measures have a positive influence in the context of a PIA.
Thank you for your attention!

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Dr. Martin Meints
Fon: +49 431 988-1226
ULD61@datenschutzzentrum.de
http://www.datenschutzzentrum.de/
References


