Biometric Technology Data Management Issues

Social Implications of National Security 2008
Suzanne Lockhart
Biometric Consulting Group

Aim

To highlight and discuss some of the significant and challenging policy, procedural and technological issues associated with supporting the proper management and administration of biometric data in large scale centralised systems.

Biometric identity management

Involves the proper management of biometric identifiers for an enrolled population in the area of:

- Registration
- Storage characteristics
- Identity assurance
- Identity protection
- Identity issuance
- Identity life cycle management
- System management

Central database considerations

- System security
- System integrity
- Reliability
- Attacks resulting in denial of service
- Auditing and reporting capabilities
- Surge capacity
- Upgrade capacity
- Disaster recovery
- Fraud reporting mechanisms

Data management

- Compile a set of comprehensive standards, policy and rules.
- Vendor and supplier rules.
- Intellectual property rights in contractual agreements

Implementation plan

- Review established goals
- Review security policies, guidelines, procedures and practices
- Classify the data
- Combine the data classification
- Define the legal obligations of the data
- Create implementation overview

Interoperability

Relates to operating in a heterogeneous environment in which policy priorities, business strategies, administrative procedures, information requirements and technology systems differ between and within agencies.

Includes three categories:

1. Business domain
2. Information domain
3. Technical domain

Data exchange & disclosure

- Proper establishment of Memorandum of Understandings
- Compliance with disclosure rules and legislation
- Privacy compliance
- Standard terms of definition

Revocation & destruction of biometric identifiers

- Formulate policy
- Revocation rules
- Revocation maintenance
- Appoint revocation administrator

Data integrity and pollution

- Progressive and slow degradation of data is a common problem which can be difficult to control. This can effect confidence in the accuracy of the data or the database generally.
- Establishing authenticity of biometric data is crucial.

Access, alteration & deletion

- Establish stakeholder policy
- Separation of duties
- Least privilege rules
- Identify and classify users based on risk
- Construct a permission matrix
- Log & audit
- Classification of data
- Access rules for third parties
- Staff training compliance with organisational standards
- Formulate policy and procedures re FOI, Privacy and other relevant legislation

Fair & lawful processing

Legislation ensures that any processing of biometric information will be legitimate.

Be mindful that legislative provisioning may make amendments to existing purposes and consequently any disclosure of biometric information may become less clear over time.

Privacy

Four separate but related concepts:

1. Information privacy
2. Bodily privacy
3. Privacy communication
4. Territorial privacy

Recommendation: Ensure all agencies accessing the data undertake a PIA.

Human rights, disability and anti-discrimination issues

Generally not deemed unreasonably intrusive due to non penetration of the body however there are four criteria which may challenge this perspective:

1. Reliability
2. Proportionality
3. Presence of fall back mechanisms
4. Prior knowledge or consent– rule of proportionality or principle of purpose.

Continued

A number of principles should be observed as communicated in several international texts including:

- The Organisation for Economic Development (OECD)
- Council of Europe
- Article 29 Working Party on Data Protection (EU)
- Council of Europe
- United Nations
- European Union

Recommendation: Clearly state the principle of purpose to support biometric capture.

Liability issues

All systems, no matter how mature the technology, experience liability issues relating to:

- Performance
- Reliability
- Accuracy
- Independent evaluations
- Lack of standards
- User acceptance/human factor issues

These issues may result in:

- Failure to enroll
- False non match
- False accept
- Denial of service

Recommendation:

- Provide adequate fall back mechanisms without causing undue disadvantage, discrimination or humiliation
- Redirect issues or uncertainty to qualified staff
- Formulate policy, procedure and training which covers these issues

Security risks

The basic principle is that the higher the security risk to higher requirement for security quality (security assurance).

Factors which increase the risk include:

- Scale and complexity of the system
- Number of users
- Number of likely enrolments
- Security sensitivity of the data
- Connectivity to the internet & other databases
- Nature of the data being stored

Security of information

Secure identity management is the application of corporate policies onto enterprise systems in a way that gives people access to the right business system resources at the time without jeopardizing the integrity and security of those resources.

Evidentiary issues

Organisations need to be confidant that records created, stored, processed or transmitted electronically will be of evidentiary value if referred for investigation or prosecution.

Three types of IT evidence:

1. Records that are computer stored
2. Computer generated records
3. Records that are partially computer generated

Continued

The IT system should be capable of demonstrating:

- Authenticity
- Reliability
- Time and date
- Identity of the author
- Safe handling and custody of the evidence

The evidence must be both technologically and legally robust to maximize its evidentiary value.

Departmental policy & procedure should include rules relating to:

- Safe handling & retention of evidentiary records
- Maintain of a log recording access and handling of evidence
- Provision of expert evidence opinion or report

Auditing and reporting

Effective auditing gives the organisation the ability to:

- Ensure policies are enforced that supply the quality of service demanded by clients, employees and business partners.
- Comply with internal and external regs and legislation.
- Mitigates the risk of litigation by producing evidence trails.
- Demonstrates compliance and adherence.
- Provides the ability to report and monitor events in real time to track usage, report and solve problems asap.
- Leverage off the data in a variety of ways as required.

Difficulty:

- Audit load and analysis capability – volume will dictate the requirement for automated/semi automated methods.

Conclusion

Major challenges discussed today:

- Systems & information security; modification rules, privacy, safety, data exchange, disclosure, audit capabilities, liability & evidence.
- Disability & extraordinary issues
- Systems integrity & protection
- External & internal attacks
- Systems capability to respond to technical, policy, social and security environment changes
- Organisational training
- Internal & external systems integration and interoperability (whole of government)
- Accurate & consistent audit and reporting mechanisms
- Effective & considered use of national/international standards

Conclusion

Biometrics can be utilised as a piece of the overall decision support system that assists verification and authentication systems.

However a concept of operation, which embodies the people, policies and technology required to achieve this goal should be developed. This should include a process framework, which links the issues presented today with the technological function of your organisation, existing legislation, policy and the over arching business strategy of your agency.

Thank you

Suzanne Lockhart

Biometric Consulting Group

Ph: + 61 (0) 419545638

E: suzanne@biometricconsulting.com.au

W: biometricconsulting.com.au