Privacy and Security in Biometrics:
Biometric Problems, issues and opportunities

Walter Scheirer, Ph.D.
Director of R&D, Securics Inc.

and

Terrance E. Boult, Ph.D.
El Pomar Professor of Innovation and Security
University of Colorado at Colorado Springs

and

Founder & CEO, Securics Inc.
Outline

- Asymmetry Impacts
- Privacy vs Security Models/Issues
- Biometrics Dilemma
- Privacy Issues for biometrics
- Some Issues to consider
Asymmetry of power

Just because we could do it (and some customers would buy it) does not mean we should.

We should avoid “Moral Hazards” inherent in asymmetric positions/markets.
Market Failure Under Asymmetric Information

In 1970, George Akerlof, published

The Market for "Lemons": Quality Uncertainty and the Market Mechanism

The Quarterly Journal of Economics,
Vol. 84, No. 3. (Aug., 1970)

It won him the 2001 Nobel Prize in Economics
Lemon Markets

Criteria for a lemon market

1. Asymmetry of information
   - buyers cannot accurately assess the value of a product through examination before sale is made
   - sellers can more accurately assess the value of a product prior to sale

2. An incentive exists for some sellers to pass off a low quality product as higher quality

3. Sellers have no credible disclosure technology (e.g. sellers with a great car have no way to credibly disclose this to buyers)

4. Deficiency of effective public quality assurances (by reputation or regulation)

5. Deficiency of effective guarantees / warranties
Fixed quality Lemons market

- Many potential buyers/sellers
- Buyers are willing to pay
  - $1,000 for low quality (lemon)
  - $2,000 for good quality product
- Only two possible equilibrium:
  - Only lemons sell, and at a price equal to the value that buyers place on lemons (bad drives out good)
  - All products sell at average price, e.g. $1,500 in the example. Sellers of good products are effectively subsidizing sellers of lemons.
  - Either market is inefficient and collapses.
Lemons market with variable quality

- In the long run choice is not just sell or not, firms can vary quality of their products
- If asymmetric market:
  - all goods sell at about the same price
  - raising your quality raises price and either raises average price of all firms or cuts your profits
  - This provides inadequate incentive to produce high quality, but more incentive to “sell well”
  - Market still fails because social value of raising quality is outweighed by uncertain information
Avoiding market failure

- The primary tenants of “asymmetric information” (and other standard IT economic models) apply in biometrics and security. It **will** likely happen in biometrics/ security if left to basic market forces.
- To provide improved value to society (and avoid market failure) we need to push for “equalization of information” and limit “lock-in” to existing systems.
Outline

- Asymmetry Impacts
- Privacy vs Security Models/Issues
- Biometrics Dilemma
- Privacy Issues for biometrics
- Some Issues to consider
Privacy vs. Security/Utility

An Inherent TRADE-OFF?

Security
Privacy

Deterrents
Accuracy, Efficiency, Usefulness

Identity protection,
Attribute protection,
Limit Logical inference,
Limit Statistical inference,
Limit abuse
Privacy risks determined by:

- Usage/collection methods – (covert or intrusive)
- System model – storage and security of data
- Unique identifiers
- Function creep
- Potential for reuse
- Potential for tracking
- Capturing/linking extra data – health, racial, disability, emotional …
- Ability to validate/challenge data
- System inaccuracy – false acceptances or rejections
Nymity (Identifiably)

Measures the degree to which information is personally identifiable or recoverable.

<table>
<thead>
<tr>
<th>Anonymity</th>
<th>Non-Reversible Pseudonymity or Polynymity</th>
<th>Reversible Polynymity</th>
<th>Reversible Pseudonymity</th>
<th>Verinymity</th>
</tr>
</thead>
</table>

The quality or state of being unknown. without name

from Greek pseudonumon, neuter of pseudonumos, falsely named
And poly meaning many, with polynymity meaning many named

from Latin verus, true, truly named

Biometrics can be almost anywhere on the spectrum:

Anonymous verification with respect to a particular token/bar-code

DeDuplication only requires system unique pseudonymity within system

Non-repudiation requires reversible polynymity, where some (trusted) party controls the reversibility
Linkability

This metric requires \( n \) data elements. Where \( n > 1 \).

Measures the degree to which data elements are linked to each other. (Identity measurement can be thought of as the degree to which data elements are linkable to the verinym or true name of the data subject).

Non-linkability

It cannot be determined which set of transactions belong with each other.

Example: Transactions belonging to the same individual.

Linkability relations can be directional, given A can link to B does not mean that B can link to A

Full Linkability

It may be fully determined which set of transactions belong with each other.

Note linkability need not be just the biometric, e.g. a smart-card + biometric may be linkable because of the unique ID in the smartcard.
Observability

Measures the degree to which identity or linkability may be impacted from the use of a system.

**Non Observability**

Nothing can be inferred from the record of the use of a system.

No record is made of the use of resources, location or transactions.

**Full Observability**

Identity or Linkability can be inferred from the record of the use of a system.

Full audit record is made of the use of resources, location or transactions.

Observability is also a function of who is considered, e.g. a transaction may be fully observable to system owner but have limited observability to another organization.
Security vs. Privacy

- Accountable to Commander, President or Board of Directors.
- Access and use controls defined by the system owner.
- Generally focused on protecting against “outsiders”.
- Short term risk based assessment. (How likely is it?)

Longer-term security and privacy share more.. If my security is impacted by another group I lose the control and other groups insiders are my outsiders.

- Accountable to the subject of the data.
- Access and use controls defined by design, use limitation, subject consent and legislation.
- Requires protecting against outsiders, insiders and system owner.
- Long term capabilities based assessment. (Is it possible?)
Security is a foundation to Privacy

- User control/consent and Fair Information Practice (not FIPS)
- authentication
- data-integrity
- confidentiality
- non-repudiation?

No matter how excellent security may be, it is never, in and of itself, sufficient to ensure privacy
Outline

- Asymmetry Impacts
- Privacy vs Security Models/Issues
- Biometrics Dilemma
- Privacy Issues for biometrics
- Some Issues to consider
What is driving Biometric System adoption?

- Law enforcement
- Terrorism and resulting Government programs such as e-boarders
- Programmatic Authentication – efficient fraud reduction
- Physical Security
- Information Security
- User Convenience
- Technology developments
- Cost – cheaper and cheaper
The Biometrics Dilemma

Alice uses Biometrics at work

Enrolled at DMV

And at the Grocery

Biometric School lunch

Fingerprint “Fun pass”

Biometric Gym Access

Hacked or Sold!

Libraries

Fingerprint “Punch clock”

Who’s the weak link in your security chain?

Sensitive Data
Biometric Privacy Pains

- 2002 UDOJ poll, 88% of biometric users concerned about misuse of personal biometric data. However, 80% support use to prevent crime.

- Biometric architectures use cyber-security to protect data, but still must trust “owner” to keep it private. Function creep (like SSN) explicitly feared. So is linking across databases.

- With > 400M PII records “lost” in US since 2005, CyberSecurity is not enough.

- Current Biometrics are permanent features. If DB is shared, compromised, and/or “acquired” the loss is permanent.
Unfortunate Privacy truisms:

1. Most people don’t value their privacy until it is threatened/lost

2. Once invaded/lost, you will need to regain your privacy over and over and over again…
Competing views on Biometrics

“Simply put, it’s getting harder and harder to preserve personal privacy without using biometrics…”

Richard E Norton, IBIA

“…Biometrics are among the most threatening of all surveillance technologies, and herald the severe curtailment of freedoms, and the repression of ‘different thinkers’, public interest advocates and ‘troublemakers’.”

Roger Clarke
Biometrics – the benefits to individuals and society

- privacy enhancing capabilities
- efficiency
- convenience
- improved access
  - remote, disability (bringing the marginalised back into mainstream)
- Improved security if done properly
Biometrics Privacy Problems

- Unique Identifier
- Infrastructure for Surveillance
- Consent/Control
  - Infrastructure
  - Template Storage
  - Biometric Acquisition
  - Usage
Privacy and Biometrics (as generally sold today)

- Claims of “privacy” since cannot recover fingerprint from template
- Government Officials Statements that biometrics are public information
- Border/Passports and National ID
  ± Biometric access control to facilities
  ± Biometric for computer/file access and data encryption
  ± Personal/home biometric devices
Vendors False Claims

Cappelli et al. PAMI, Sept. 2007

1) Selection of the singularities

Average successful attacks against nine different systems

- 81% high security

Templates ARE effectively invertible!
And it keeps getting better. (e.g. Jain-et-al ICB 2009)
Security by Obscurity is not Real Security

- Many people think that a security system becomes more secure if its internal structure is secret
  - Example: A secret encryption algorithm
- The exact opposite is the case
  - Secret systems can only be analysed by a few internal specialists and are more likely to be insecure.
- Kerckhoffs’ principle
  - The security of a cryptographic system shall always and only depend on the secrecy of the key. Everything about the algorithm except for the keys shall be open
- Bruce Schneier’s extension:
  - "Kerckhoffs' principle applies beyond codes and ciphers to security systems in general: every secret creates a potential failure point. Secrecy, in other words, is a prime cause of brittleness—and therefore something likely to make a system prone to catastrophic collapse. Conversely, openness provides ductility."
Outline

- Asymmetry Impacts
- Privacy vs Security Models/Issues
- Biometrics Dilemma
- Privacy Issues for biometrics
- Some Issues to consider
Why Technology for Privacy

- Policies to protect privacy must be followed by everyone to be effective. They are important, but technology can add confidence that policies are being followed.
- Policies “evolve” to allow/support function creep
- Biometrics are long lived data and once privacy is violated its hard to “fix”.
- Biometrics can be abused without our knowledge
- If we help build the technology, its our social responsibility to make sure it is used properly.
- Given more technological choices we may simultaneously increase privacy and improve security.
Different Approaches to Privacy

- Central Repository/Decision Model – Fort Knox syndrome
- Divide and Conquer – strategic pseudonymisation/anonymisation
- Build in elements of personal Consent and Control to process
- Smart Hardware
  - Privacy Rules Embedded in Hardware
- Smart Data