

***Help! My Biometric Has Been
Stolen...***

Russ Ryan
National Biometric Security Project

Biometrics/Privacy Evolution

- Biometrics authenticating increasingly diverse demographic segments
- Privacy becoming more of an issue
- Common storage of biometric and biographic data becoming problematic
- We increasingly face the sometimes daunting task of protecting that personal information

U.S. Privacy Act of 1974

- No federal agency can disclose personal information to another federal agency or person without prior written authorization
- Federal agencies are allowed to request an exemption, if they are involved in law enforcement or national security defense
- The Central Intelligence Agency, for example, is expressly exempt from the law

GAO Report on PII

- Personally Identifiable Information – PII: any information that can be used to distinguish or trace an individual's identity, such as:
 - name
 - SSN
 - date and place of birth
 - mother's maiden name
 - ***biometric records***
 - and any other information that is linked or linkable to an individual.

Current Situation

- Cost of identity fraud in transactions continues to grow
- Traditional ID databases design proving problematic
 - **central databases lead to social/political/economic issues**
- Key to solving the problem is separating the core authenticator – a biometric – from all of the personal information. This has not been achieved to date.

Willingness to share identification records within organizations/agencies & especially with external organizations/agencies is severely limited

Evolution of Anonymous Authentication

Identification

I know you

Identity Management

I know all about you

Anonymous Authentication

I know who knows all about you

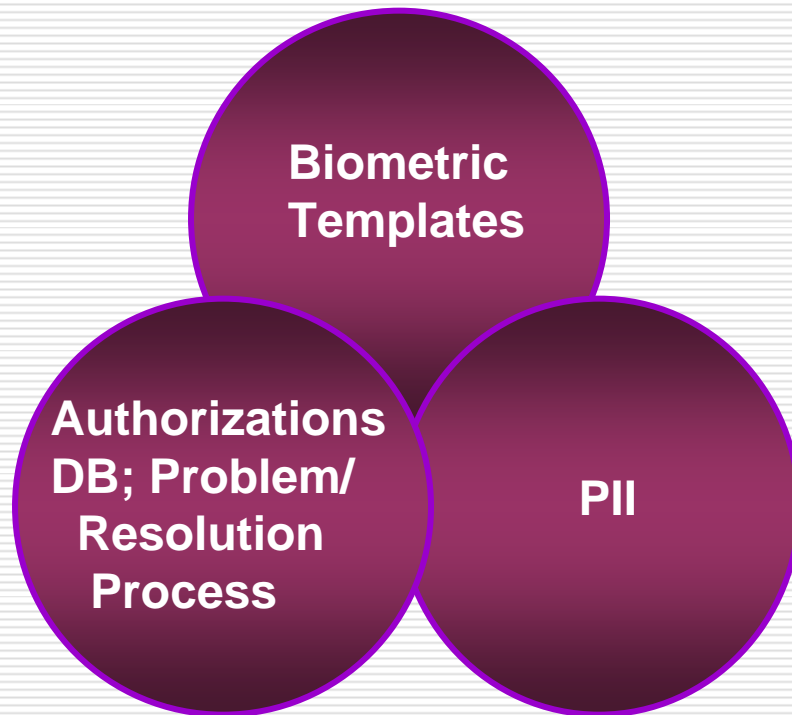
A Systems Perspective Companion to the

BIOMETRICS IN SUPPORT OF PERSONNEL IDENTITY (BSPI) WHITE PAPER



NBSP

Biometric ID Management Today



- Integrated DB of Biometric/Biographic & Authorization Data
- Biographic data vulnerability increased

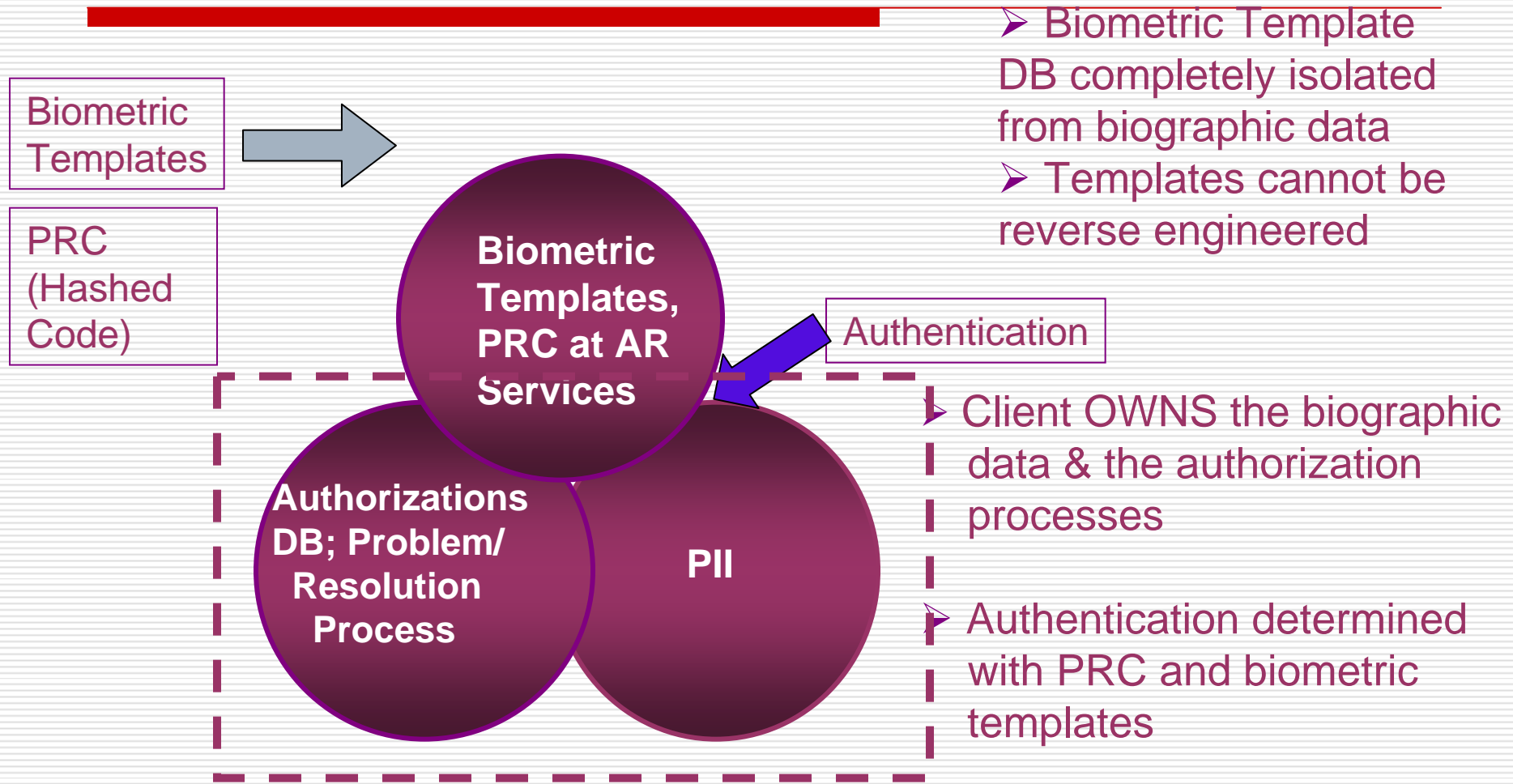
What Is Anonymous Recognition?

- Biometric authentication of identity in an anonymous operation
 - **Biometrics & encrypted code completely isolated from PII**
 - **Multiple biometrics can be used**
 - **Ownership of identity within the process retained by subscriber**
- Multiple subscribers/owners can access and use the AR process without sharing proprietary information

Development of Concept

- **NBSP Ahead of the Curve**
 - **Anonymous recognition concept first discussed here in 2006**
 - **Past two years financially seeded the idea; worked with technology partners and patent now pending**
 - **Difficult to secure investment w/o market need**
- **Interest has begun to emerge**
 - **DoD has highlighted benefits of anonymous recognition in a white paper**
 - **Joint U.S./select EU countries investigating anonymous recognition for border automation data sharing**
 - **Currently defining a license agreement with a major integrator to build first platform in 2009**

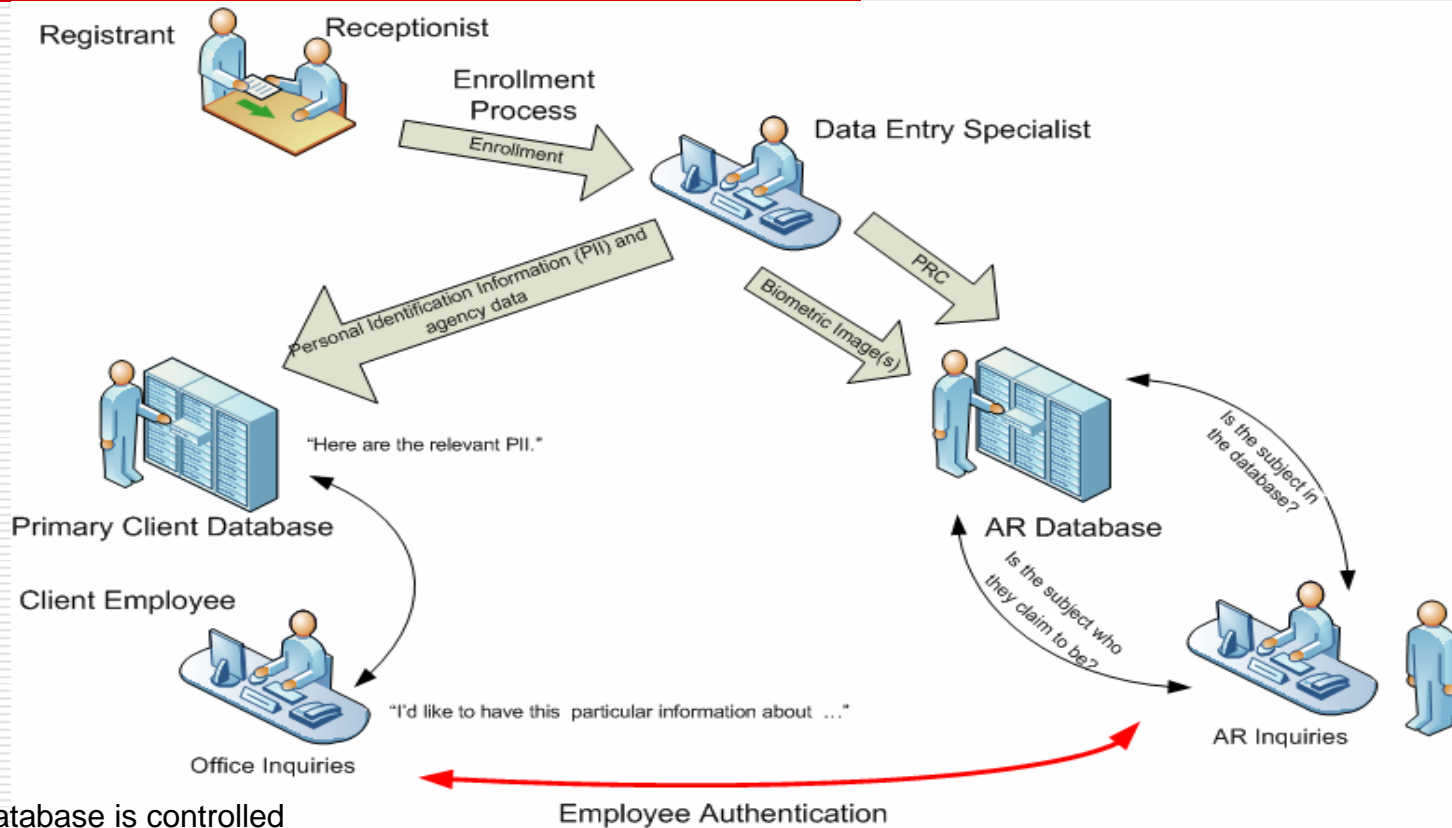
The AR Concept



AR Enables...

- Highly reliable authentication of identity in complete isolation from personal and private data
 - **No user name/pins/or passwords**
 - **No SSAN**
 - **No name or address**
 - **No compilation of usage data**
 - **No access or reporting unless pre-approved**
- Organizations with common goals to share a common authenticator-not common data
 - **Use with multiple, separately owned databases, allowing common communication without sharing proprietary data**
 - **Authentication unlocks access to pre-approved sources**
 - **An alternative to concerns about a national ID card**

AR Enrollment Process



- Access to database is controlled
- Data are encrypted
- Access to PII data is based on 'need to know.'

Many tasks can be effectively satisfied by answers to these two questions.

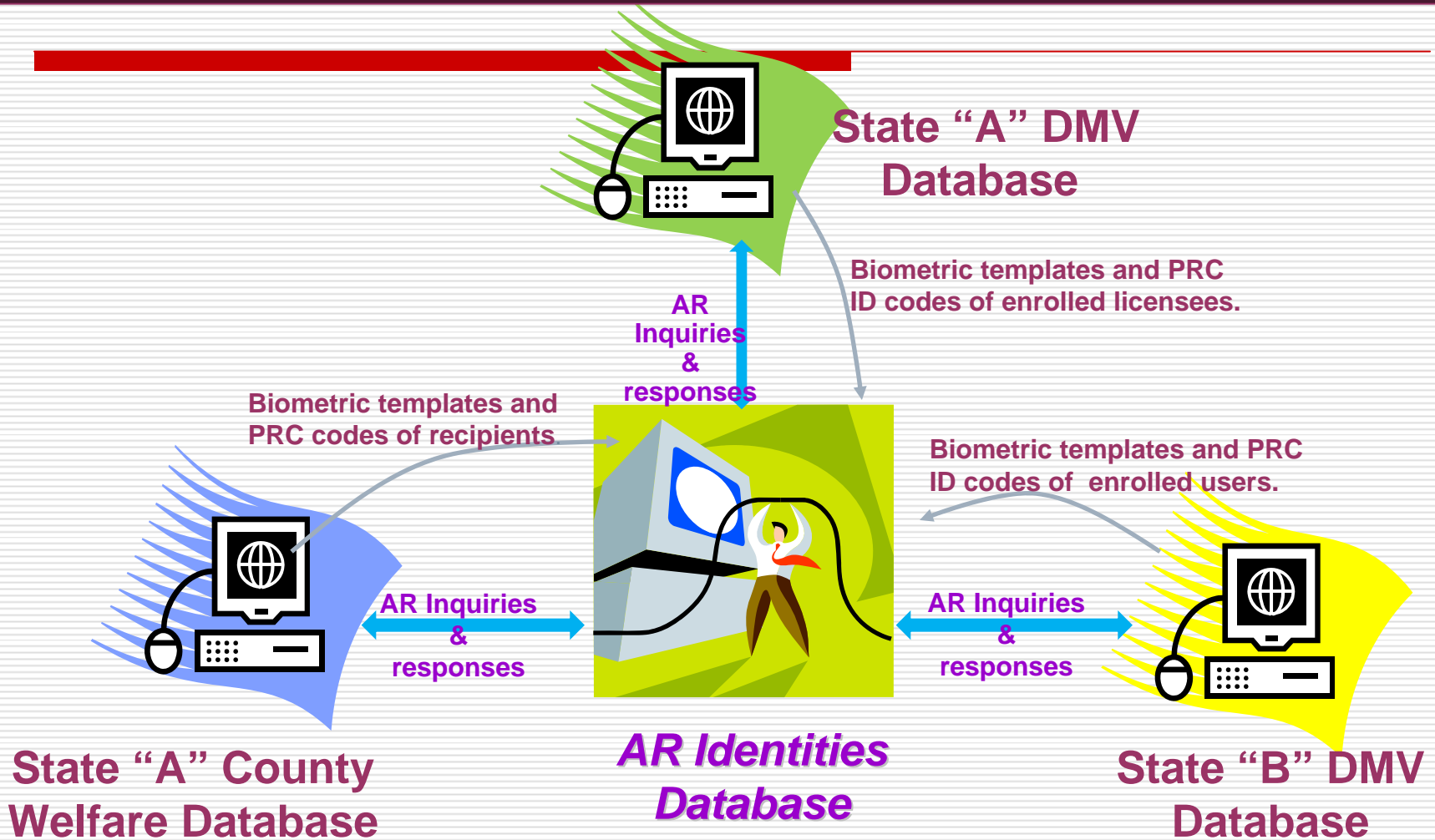
AR Enrollment Process Reveals

- If the individual is enrolled in the database
- The organization of enrollment or registration
- If the submitted biometrics match the PRC
- If they match...identity is confirmed
- If they don't match, AR will distinguish the event as:
 - **Attempted Identity Creation for Fraud (creating a new ID)**
 - **Identity Theft (stealing an existing ID)**

Generic Applications for AR

- Bridge databases with diverse structures and owners without compromising private, personal, or sensitive information
 - **Multi-State Licensing Validation**
 - **Various Health-Care Providers for Insurance Validation**
- Verify the identity of persons in large, geographically dispersed organizations
 - **Government field operations**
- Block attempts at identity fraud or theft
 - **Government benefit programs**

An AR Solution Example



Keys to Success

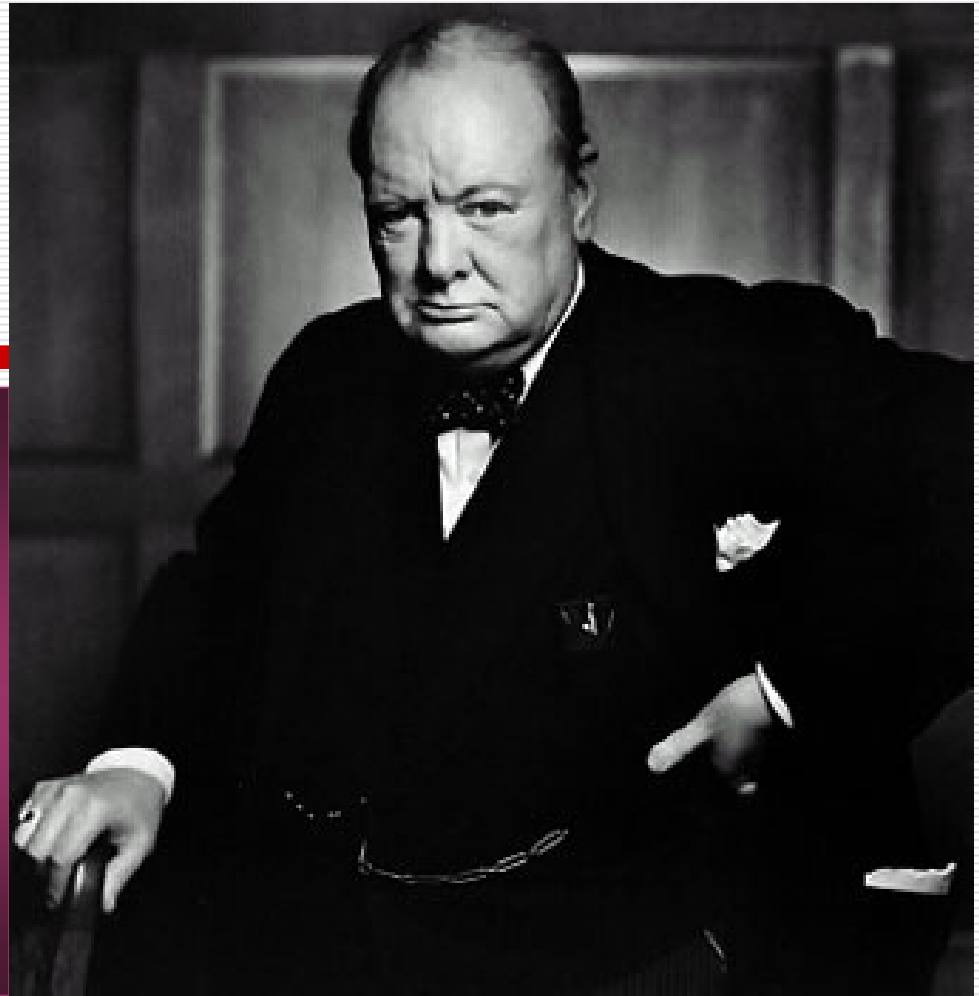
- **Multi-modal matching capability**
 - **Accommodates legacy databases**
 - **Does not restrict subscriber to a specific modality**
 - **Enables biometric fusion if applicable**
- **Certified performance capability of biometric products**
 - **Products must meet stated performance thresholds**
 - **Thresholds can be verified by controlled performance tests similar to Qualified Products List (QPL) test process**
- **Independent, trusted service provider**
 - **Reduce vulnerabilities**
 - **Minimize exposure**
 - **Provide assurance of privacy to employees**

AR Benefit Summary

- Preserves database integrity by providing a bridge between databases controlled by different states, agencies, or other entities without sharing PII
- Enables authorized access to other applications and databases of personally identifiable information
- Isolates the confirmation of identity from the requiring transaction

- ❖ ***Increases protection of PII in ID authentication process***
- ❖ ***Begins to eliminate information silos by neutralizing hesitancy of organizations to share information***

He may be one of
the most famous
and recognizable
people of the 20th
Century.....but...



AR Would Know Him Only As.....



**A biometric Image
+
A Personal Reference Code**



Russ Ryan

rryan@nationalbiometric.org