PANEL

Privacy and Legal Issues in the Collection, Distribution, and Use of Biometric and Forensic Datasets

Lessons Learned

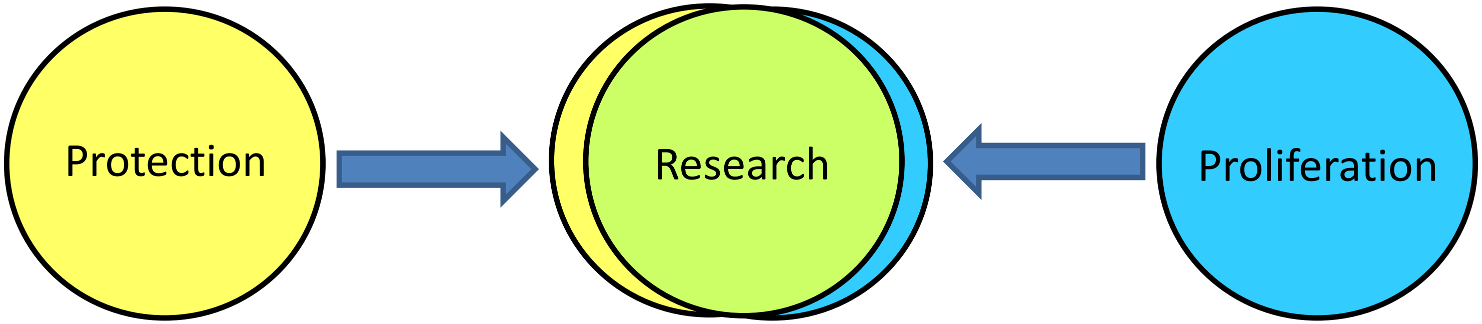
Michael Garris
Biometrics Senior Scientist
NIST/ITL/Information Access Division

Introduction

- Biometrics Research Manager (for 7 years)
  - Facilitated human subjects determinations
    - Pursued legal clearance to use specific biometric datasets for NIST research
      - Standards Development and Technology Evaluation
  - During a period of institutional change regarding policy practice of the Common Rule
  - Asked to share “Lessons Learned”

What’s our goal?

- Protection of human research subjects
  - No physical or psychological harm
  - No infringement of rights (e.g., privacy)
- Proliferation of data samples to support open research



Conundrum #1

- *Biometrics are not secrets*
- How should this factor into human subjects protection policies?

IRB Documentation (1 of 4)

- Required Elements
  - IRB Application / Project Description
  - Protocol
  - Consent Form
  - Letter of IRB Approval

IRB Documentation (2 of 4)

- *LESSON: IRB Documentation will be used by outside organizations*
  - Scrutiny, requirements, & process vary by research organization
  - Requires tight document control
    - Use highest standards for drafting and maintaining documents
      - Linking current versions of the Required Elements (prior slide)
      - Documenting updates (e.g., increase in # subjects)

IRB Documentation (3 of 4)

- Data User Agreements
  - Often required with research datasets
    - + Should be as light weight as possible
    - + With a process for adaptation (some flexibility)

IRB Documentation (4 of 4)

- Improving the Situation
  - – With cross-organization differences in scrutiny, requirements, and process ...
    - + At the highest level of legal authority and credibility (HHS/OHRP?)
    - + And specifically for Biometrics
    - = Publish standard templates and best practices for IRB documentation

Two Types of Biometric Samples

1. Collected for Research Purposes
   - In Laboratory
   - Requires an IRB
   - Data is publically available
2. Collected for Operational Purposes
   - In Field
   - Never will involve and IRB
   - Data is controlled and often sensitive

- The Gap
  - Significant qualitative difference between these two sample populations
  - Negatively impacts algorithm development, particularly involving machine learning methods

Strategies for Operational Data

- Making operationally collected data available for research purposes
  - + Determine authority for sharing the data
    - Often to improve the capabilities to meet an agency's mission
  - + Privately Code / De-identify / Anonymize the data samples
  - + Restrict distribution and ensure data protections via strict Data User Agreements
  - = A determination of "No Human Subjects Research" is possible

Face Photos – a Challenge

- Common Rule holds face photos to a higher standard
  - We recognize each other by our faces
- Overcoming the Hurdle
  - Tighter access control
    - Lock down the data both physically and logically
  - Disable online/external search and export services
  - Policy, procedures, & training
    - To handle rare cases when researcher recognizes a subject

Conundrum #2

- *Biometrics Research is evolving into Human Identity Research*
- Requires:
  - Multiple Biometric Modalities
    - (e.g., fingerprints + face photo + iris images + ...)
  - Soft Biometrics
  - Biographic Information
- How should this factor into human subjects protection policies?

Summary

- 2 Conundrums
  - *Biometrics are not secrets*
  - *Biometrics Research is evolving into Human Identity Research*
- IRB Documentation
  - Remember other organizations will use your documentation
  - Legally recognized standard templates and best practices would be helpful (HHS/OHRP?)
- Laboratory and Operational Data
  - Both are important
  - Managed differently