



THE CENTER FOR ADVANCED STUDIES  
IN SCIENCE AND TECHNOLOGY POLICY

# TECHNOLOGY, POLICY, AND CULTURAL DIMENSIONS OF BIOMETRIC SYSTEMS: INFORMATION SHARING



**KIM TAIPALE ([HTTP://TAIPALE.INFO](http://taipale.info))**

EXECUTIVE DIRECTOR, CENTER FOR ADVANCED STUDIES  
SENIOR FELLOW, WORLD POLICY INSTITUTE

PRESENTED AT:

**BIOMETRICS SYSTEMS: WORKSHOP  
NATIONAL ACADEMY OF SCIENCES**

WASHINGTON, DC • MARCH 16, 2005

# Center for Advanced Studies

<http://www.advancedstudies.com/>

- *Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties*, in *21st Century Information Technologies and Enabling Policies for Counter-Terrorism*, Robert Popp and John Yen, eds. (IEEE Press, forthcoming 2005) <<http://policy-appliances.info/>>
- *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd*, 7 Yale J. L. & Tech. 123 (Dec. 2004) <<http://ssrn.com/abstract=601421>>
- *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 Colum. Sci. & Tech. L. Rev. 2 (Dec. 2003) <<http://ssrn.com/abstract=546782>>

## Presentation overview: underlying themes and info sharing

- Technology and policy
- Biometrics and systems
- Biometrics as identifiers (to establish a CI for data attribution)
- Biometrics as identifier begs the question of the purpose for identification and ID systems
- Cannot evaluate biometrics independent of the purpose and context of the policy and the system
- Policy issue is not biometrics but data use and information sharing in a digital information environment
- Suggest some principles

# Technology, Policy, and Culture

- Any security system is a social construction (technology, legal, political, cultural, market, etc.) (wicked problem)
- Technology constrains policy as much as policy sets requirements for technology development
- Technology development process is an iterative process between business process needs and technical capability
- Technologists need to inform policy makers about what is possible and policy makers need to inform technologists about purposes or business process needs (not presumed technical requirements or specs)
- Note: the word “biometric” appears 35 times in the Intel Reform Act (note also, “metadata” in EO13356, SHARE in Intel Reform)

## Error rates and policy

- Match CI/error rate to policy needs or use in particular application
- Cf. zero error (technical issue) vs. risk assumption (policy issue)
- Cf. technology (tool) vs. system (application)
- Design for elegant failure (systems AND policy)
- Cf. layered security (dependant variables) vs. ensemble security (independent variables) (use both strategies to reduce risks)
- “close enough for government work” - focus on preventing catastrophic outcomes and reducing national security threats

# Biometrics and systems

- Confidence interval for use of biometrics in a particular application is a function of the weakest link in the system
  - Enrollment
  - Measurement
  - Verification
  - Human factors (70% of attacks from insiders)
- Systems are subject to
  - Errors, breaks, and compromises (see also Swire article about when (and when not) secrecy of standards is the appropriate security strategy)
  - Counter-programming and attacks (note that statistical techniques are particularly susceptible to attacks)
  - Technical choice will determine effectiveness of security feature, e.g., detecting for liveness at verification vs. detecting for non-liveness
    - Easier for attacker to emulate liveness than circumvent non-L detection

“Biometrics” may be the strongest link ...



... but consider the application

# What's the purpose or need for using biometrics?

- Is there a need for better “identification”?





## What's the purpose? (cont.)

- A need for better identification?
  - 19 hijackers and their ID
    - 9 hijackers had 11 (not 63) licenses (2 duplicates)  
***in their real names and validly issued***
  - Failure was not identification but watch list matching and information sharing
  - Query: is biometrics a solution to these failures?

(see related, "*Not Issuing Drivers Licenses to Illegal Aliens is Bad for National Security*")  
Press Release 12/2004 available at <<http://alien-ID.info>>)

## What's the purpose? Do I need "papers" to prevent ID theft, and, if so, what kind?

- 1:1, to prove who you are (Traven, *Das Totenschiff* 1926, *The Death Ship* 1934):
  - “You ought to have some papers to show who you are.”
  - “I do not need any papers. I know who I am.”
  - “Maybe so. But others are also interested in who you are.”
- 1:N, the system tracks who you are (T. Gilliam, *Brazil*, 1985):
  - “Do you want to see my papers?”
  - “No need, sir”
  - “But I could be anyone.”
  - “No you couldn't, sir, this is information retrieval.”
- In 1:1 case subject retains control and security of reputation (and the individual has the most incentive to prevent ID theft) vs. 1:N where attribution and control of reputation is by (and for benefit of) third parties (question is when is which required and/or appropriate)
  - Rules for managing reputational elements and matching system to needs
  - Transience, proximity, error correction, who decides?
  - A system in which biometrics are aggregated in DBs and sold is no more secure against ID theft than one that aggregates and sells SSNs (in any case, encrypt biometrics!)

# Purposes of identification systems

(see also, "Presentation: Who's Who in Whoville" 01/2004 <<http://whoville.us>>)

- To enforce rules in a system by authenticating "identity" for
  - Authority - permission to do or not do something (e.g., access control) (default state: deny > totalitarian), or
  - Accountability - responsibility for actions w/in the system (default state: presumption of innocence > freedom)
- Are these purposes/rationales useful against disposable actors?
  - Israeli experience <12 hrs between recruitment and strike
  - Suicide attackers w/ no sanctionable support structure
- Applications that make sense for biometrics are those that improve on current needs/methods for ID. Biometric technology should not itself be the rationale for developing new ID systems.
  - Verify identity (1:1) vs. new req. for primary identification (1:N)
  - e-passports, drivers license, employee ID, etc.

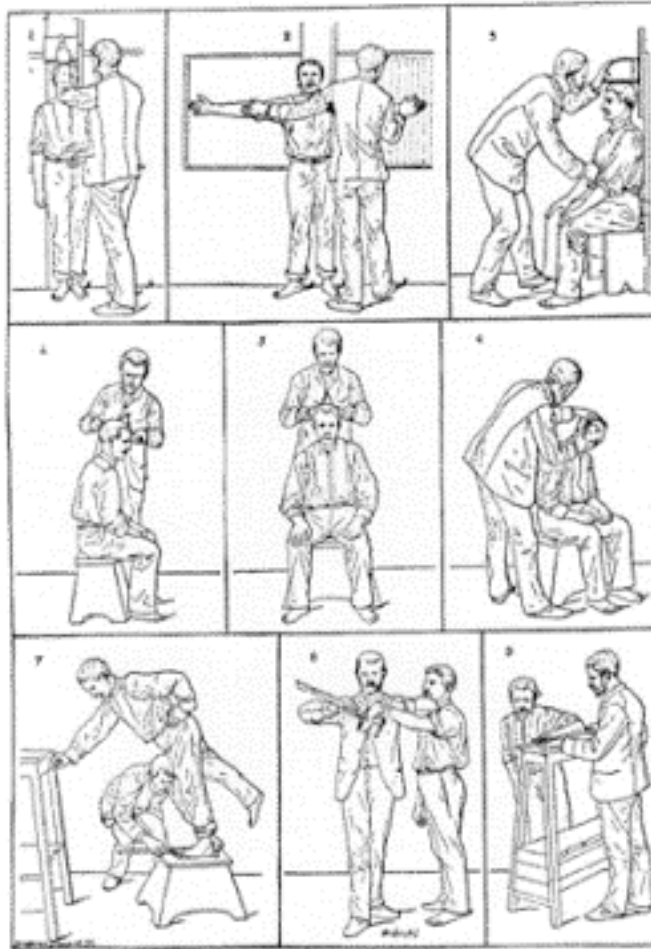
## Purpose of using an identifier (verifying ID or attributing data)

- Link an individual to data with a certain degree of confidence
  - Attribute individual > knowledge of identity or behavior (reputation)
  - Cf. data mining (data/reputation > identity or individual)
- Thus, the policy issue is not just the accuracy or CI of the identifier (or biometric) but how useful the linked “data” (watch list, authorization, reputational factors, etc.) is for decision making within the particular system and desired policy outcome
- 1:N screening is a brittle security strategy that doesn’t scale well
  - Watch list problems
    - Varied criteria for inclusion, diffuse responsibility for integrated list, and dilution (16/2001 > thousands/2002 > 200K/2004 > ?)
    - See also “Presentation: Secure Flight” 12/2004 <http://secure-flight.info/>
  - Trusted systems problem (can’t catch unknowns w/ screening)
    - Good guys, bad guys, and not yet proven bad guys

# An [abridged] history of biometrics

- Markings (c. ? BC) (~ ancient Roman tattoos for prisoners and slaves)
- Handprints in China (c. 1400)
- Bertillonage (late 1800s-mid1900s) (~ modern criminology and forensics)
  - 20-60 minute measuring exam: height, length, and breadth of the head, the length of different fingers, the length of forearms, etc.
  - Combined w/ cataloging system (used to ID repeat offenders)
  - 1/286,435,456 “proven” uniqueness factor (system worked OK)
- Fingerprints (in US c. 1903- ) (note modern origin was not for ID, but used by British in India as token to seal contracts mid-1800s)
  - Adopted in US prison system in 1903 the day after identical “identification” (w/in tolerances) using Bertillonage of two Fort Leavenworth prisoners
- “Biometrics” in 21st C is really about the digitization of biometric processes, i.e., digitally enabled measurement and cataloging

## Bertillonage measurement (“enrollment”) (1890s)





## Bertillonage "template" (1890s - mid1900s)

(Ch. Brown)

Height	1m 79.6	Head l'gth	19.8	L. Foot	27.1	Circle	leh	Age	22	Born in	
Eng. H'ght	5-10 3/4	Head width	16.3	L. Mid. F.	11.2	Periph Z		Apparent Age			
Oust. A	1m 75.5	Cheek width	14.4	L. Lit. F.	8.7	leh-Mel		Nativity	Louisville, Ky.		
Trunk	94.9	R. Ear	6.8	L. Fore A.	46.6	Pecul		Occupation	Shoemaker		

Remarks Incident to Measurement



1663

**DESCRIPTIVE**

Inclu.	Reddy	Ridge	Box	Beard	Shaved
Height	M	Base	(Edu) Root	Hair	Black
Width	Brn	DIMENSIONS			Complexion
Pecul		Length	Projection	Breadth	M. Dark
		br	br	m	Weight
		Pecul			165
					Build
					M. Slim

BUREAU OF IDENTIFICATION  
Department of Police,  
Tulane Ave. and Saratoga St.  
New Orleans, La.

Measured Feb 1 1913  
By Jno. G. Harris

563

**BUREAU OF IDENTIFICATION**  
DEPARTMENT OF POLICE, CITY OF NEW ORLEANS.

NAME Hugh M. Howell Reg. No. 1663

Alias Color White

Residence Louisville, Ky. Date of Arrest Jan 31 1913

Crim. Dang & Susp. (D.P.) Held By Judge Night Recorder

Officer Det. Jno. Sabatino & W. P. Methe Precinct

Disposition of Case Feb 2/13, fined \$20. or 9 days + 30 days Parish Prison

Previous No.'s

NUM'L ORDER MARKS, SCARS AND MOLES

I Circular tattoo mark on forearm - Ant

Five faint cut scars 2" phal. indep. finger - Ex













II Tattoo of "H. M. H." & stars under cut - Ant

III Irreg. scar above middle right eyebrow

Small irreg. scar above inner point left eyebrow

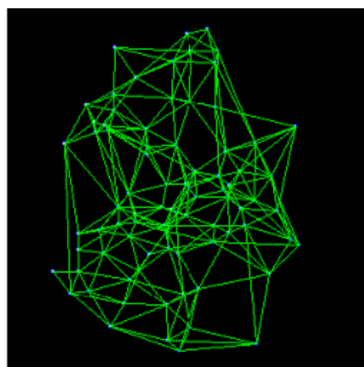
Small dark moles about the face

## Fingerprints “template” (by mid 20th C.)

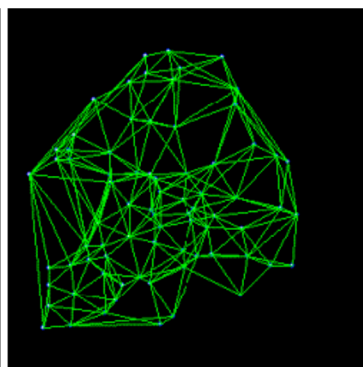
APPLICANT		LEAVE BLANK		TYPE OR PRINT ALL INFORMATION IN BLACK		FBI		LEAVE BLANK	
Leave Blank		Teacher, Theresa C.		LAST NAME NAM		FIRST NAME MIDDLE NAME		Leave Blank	
SIGNATURE OF PERSON FINGERPRINTED				ALIASES AKA		O R I		DATE OF BIRTH DOB	
RESIDENCE OF PERSON FINGERPRINTED				Formerly: Theresa Smith		NY9219402 NYSTED Dept-FPU ALBANY, NY		12/31/70	
318 School Street Hometown, NY 11111				CITY/STATE ZIP		SEX RACE DOB WEIGHT POB HOB		PLACE OF BIRTH POB	
DATE 5/01/02				SIGNATURE OF OFFICIAL TAKING FINGERPRINTS		F W 5'7" 155 Gr Bro		Ohio	
EMPLOYER AND ADDRESS (if applicable) Smart Falls Central School Dist Smart Falls, NY 11111				YES NO NA Leave Blank		LEAVE BLANK			
Leave Blank				EDUCATION Leave Blank		CLASS Leave Blank			
REASON FINGERPRINTED				ARMED DANGEROUS YES NO NA Leave Blank		REF Leave Blank			
Leave Blank				SOCIAL SECURITY NO 000-10-1111					
				RECEIVED AND FILED YES NO NA Leave Blank					
									
1. R. THUMB		2. R. INDEX		3. R. MIDDLE		4. R. RING		5. R. LITTLE	
									
6. L. THUMB		7. L. INDEX		8. L. MIDDLE		9. L. RING		10. L. LITTLE	
IDENTIX TP600 1259						ALS004228 LEX004229			
									
LEFT FOUR FINGERS TAKEN SIMULTANEOUSLY					RIGHT FOUR FINGERS TAKEN SIMULTANEOUSLY				



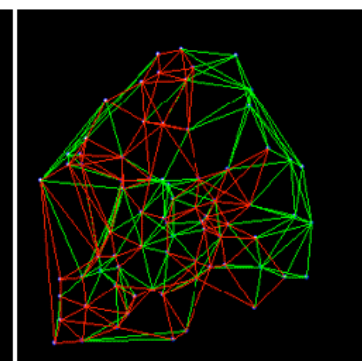
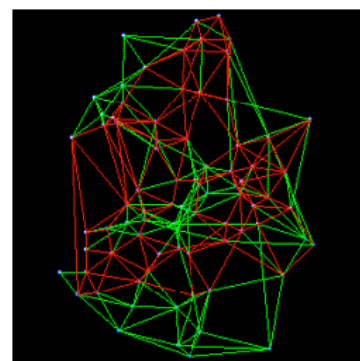
# “Biometrics” today - digital templates



Template Code 1



Template Code 2



Templates obtained from two images of the same finger with common sub-templates highlighted

and automated matching

Thus, the real issue is digital record keeping and information sharing not the use of biometrics



## Some technical issues w/ policy implications

- Factors affecting the choice of particular biometric method to use for a specific application:
  - Robustness
  - Distinctiveness
  - Accessibility
  - Acceptability
  - Availability
- Systems design issues that have both security and privacy policy implications:
  - Cooperative vs. Non-Cooperative
  - Overt vs. Covert
  - Habituated vs. Non-Habituated user
  - Attended vs. Non-Attended
  - Standard vs. Non-Standard Environment
  - Public vs. Private
  - Open vs. Closed

# Information Sharing issues

- Information Sharing issues (biometric or other ID systems)
  - Data collection (integrity, security, human factors, error correction)
  - Transmission (local vs. DB matching)  
(this is a different issue than 1:1 v 1:N)
  - Processing (transparency of algorithms and error rates)
  - Decision making (thresholds for referral) (rules for action)
  - Storage (security, transience/expiry, and proximity, etc.)  
(re-use of reputational elements)

# Privacy, power, and information control

- What is “privacy” (1st order value or 2nd order value)?
  - To secure ID information (prevent ID theft) -- 2nd order
  - To protect civil liberties through inefficiency/obscurity -- 2nd order
- Parsed privacy interests (Whalen footnote)
  - Secrecy (1st order?) (but if alienable and variable, contextual ...?)
  - Anonymity (SupCt concept of anon. is really pseudonymity)  
(no true anonymity in the “real” world)  
(see also, “Presentation: Security and Anonymity” 05/2004 <http://security-and-anonymity.info/>)
  - Autonomy (due process) (protect subject from the consequences of disclosure/knowledge through procedural rules)
- Additional Constitutional principle:
  - US DOJ v. Reporters Committee (1989)
  - Recognized a protectable right in inefficiency of information access
  - J. Stevens (practical obscurity [of reputational elements?])

# Information sharing principles

- Due process (= fundamental “fairness”) factors (~ FIPs)
  - Predicate for use of biometrics/system (CT) (~ DM) (is it effective to meet a recognized state interest -- i.e., does the problem justify the solution, e.g., does use enhance security vs. just “ID”)
  - Alternatives (and alternative/less intrusive implementations: e.g., 1:1 vs. 1:N, minimize transaction records, tracking, linking, etc.)
  - Consequences
    - Granting or denying privilege (vs. punishment)
    - “Match” is predicate for what?  
access to plane (no rules) vs. prosecution (rules)
    - Reuse/expiry of reputational elements
  - Error correction

# Proposed technology Hippocratic Oath

- First, do no harm (don't build in intrusions or features to do things that aren't necessary just because you can)
- Second, limit the harm (provide only the features and design in a particular system needed to accomplish the identified policy outcome) (observe the law of proportionality)
- Third, beware of unintended consequences
  - Don't generate transaction records unless necessary
  - Allow for policy control over re-use of data (~ transience, proximity)
  - Provide technical means to control data and information sharing
    - Smart data (metadata) and intelligent systems with intervention points to enforce policy (see <<http://policy-appliances.info>>)

# P.O.V.



Consider: is any particular application “effective” for its intended purpose?  
Does it enhance national security, security theater, or social control?



# More information

[contact.advancedstudies.org](http://contact.advancedstudies.org)

</>