THE CENTER FOR ADVANCED STUDIES
IN SCIENCE AND TECHNOLOGY POLICY

Identification Systems and Domestic Security: Who's Who in Whoville

K. A. Taipale
Executive Director
Center for Advanced Studies

Presented at:
The Potomac Institute for Policy Studies
and The Heritage Foundation Roundtable:
"The Politics and Law of Identity and Identification
in the Context of the War on Terror"
Arlington, VA • January 28, 2004

Introduction: Identifying a Problem?

- Second Markle Report, Appendix A:
  - "There is strong evidence that having reliable means of personal identification would greatly enhance many of the new security measures introduced since September 11, as well as those that were in place prior to the attacks."
- Premise: reliable ID is "essential" to security:
  - Prevalence of false/fraudulent ID is a vulnerability
- Report presents evidence of current inadequacies
  - Porosity of checkpoints (counterfeit documents get through)
  - Prevalence of false/fraudulent identification documents
  - Identifies driver's license as 'weakest link'
- Implicit problem: secondary uses

Markle Report Recommendations

- Improve the Process
  - Enrollment process (breeder documents)
  - Validation/Verification (SSN, E-Vital, uniform standards)
  - Audit trails (to prevent misuse/abuse)
- Improve the Personnel
  - Training (spot counterfeits at enrollment and at checkpoint)
  - Selection and oversight (prevent fraud or abuse)
- Improve the Technologies
  - Biometrics, smart cards, network scanning, crypto
- Importantly, the report calls for independent review of: Identification, Security and Privacy issues

Identification, Security and Privacy Issues

- What is "identification"?
- How does it impact "security"?
- What are the "privacy" implications?
- Where does "technology" fit in?
- Expose the fallacy of the dichotomous choice: "identified or anonymous"

Identification = Authentication

- Three Forms of Authentication
  - Individual Authentication (~identification)
    - **Confidence** that an identifier refers to a specific individual
  - Identity authentication (~indexing)
    - **Confidence** that an identifier refers to an identity
  - Attribute authentication (~authorization)
    - **Confidence** that an attribute applies to a specific individual

Two general purpose of authentication

- Confirm Authorization (binary)
  - Authorized to do something (or not, i.e., watch list)
    - Gain access or use resource
    - Functional equivalence (cf. MetroCard w/ Pentagon pass)
    - Authorization attribute relates to granting policies
    - Authentication requirements vary with security needs
- Provide Accountability (variable)
  - Accountable to do something according to certain rules
    - Information collected/stored to provide accountability
    - Functionally not equivalent (cf. MetroCard w/ Pentagon pass)
    - Accountability attributes and requirements vary with security need
    - E.g. ski pass -- revoke token -- "anonymous" accountability?
    - Cf. driver's license -- authorized to drive / accountable for accident
    - Cf. EZ Pass, MetroCard (secondary uses)
    - When is revelation of identity required for accountability?
    - How long is accountability information required to be held?

Methods of Individual Authentication

- Passwords
  - "something you know"
- Tokens
  - "something you have"
- Data match
  - "something you are"

The most secure methods of authentication combine all three methods

- Reveal a password - e.g., PIN
- Present a token - e.g., ID Card
- Match data
  - The token is authenticated
  - The token is matched biometrically to the subject
  - The password is verified (data base or smart card)
  - The behavior is matched against a profile (deviation analysis)
  - (The subject can also be biometrically matched directly to data base)

Use of authentication

- Authentication is employed when control of access and/or protection of a resource is required
- Query: When, where and by what method is authentication appropriate and/or constitutional in a democratic state?
  - What predicate is necessary before requiring individual identification? (Hiibel v. Nevada)
  - What activities require permission/authorization? (Gilmore v. Ashcroft)
- Policy goal: determine the calculus of reasonableness that relates purpose and method of authentication to the security need and the privacy intrusion
- Technology goal: provide technical features to support policy

Real Problem of Identification Systems in Domestic Security

- Using authentication systems for secondary purposes undermines integrity of system
- E.g., driver's license as ID for financial transactions results in the value for false/fraudulent ID exceeding the investment value in "secure" driver's license (~domestic security)
- E.g., SSN
  - Used as both a general identifier (college ID, driver's license, etc.) and as password/verifier
  - Result: identity theft is trivial

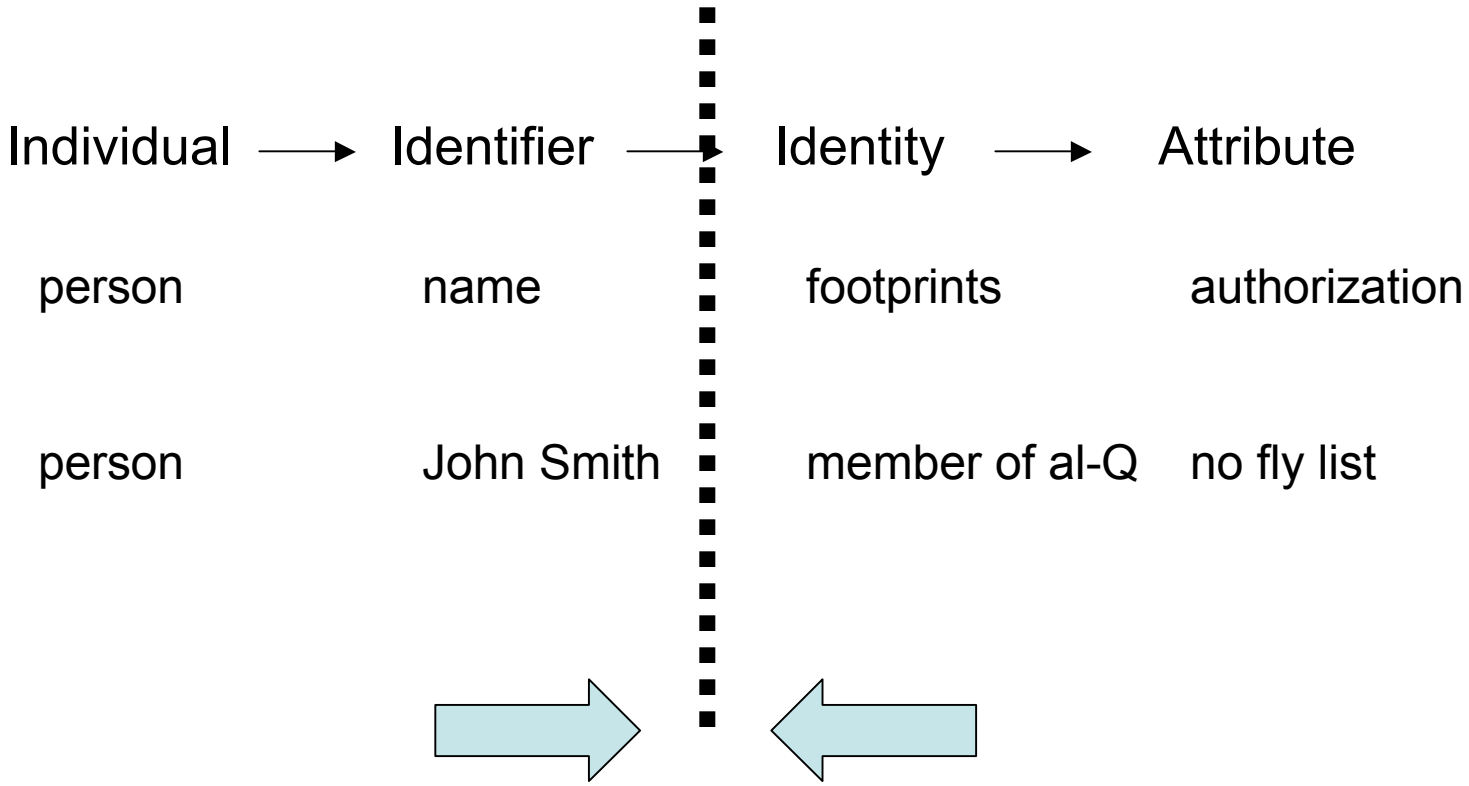
Additional Problem in Domestic Security: A Trusted Systems Problem

- What does identification add to security?
- There is no way to prove that you are trustworthy, best you can do is prove you are not "not-trustworthy" (i.e., not on watch list)
- That requires that the attribute of "not trustworthy" has been correctly pre-determined (list criteria)
- Watch list vs. no-fly list (allocate resources or deny liberty)
- The question is what is the default status:
  - Innocent until proven guilty (freedom)
  - Guilty until proven innocent (tyranny)

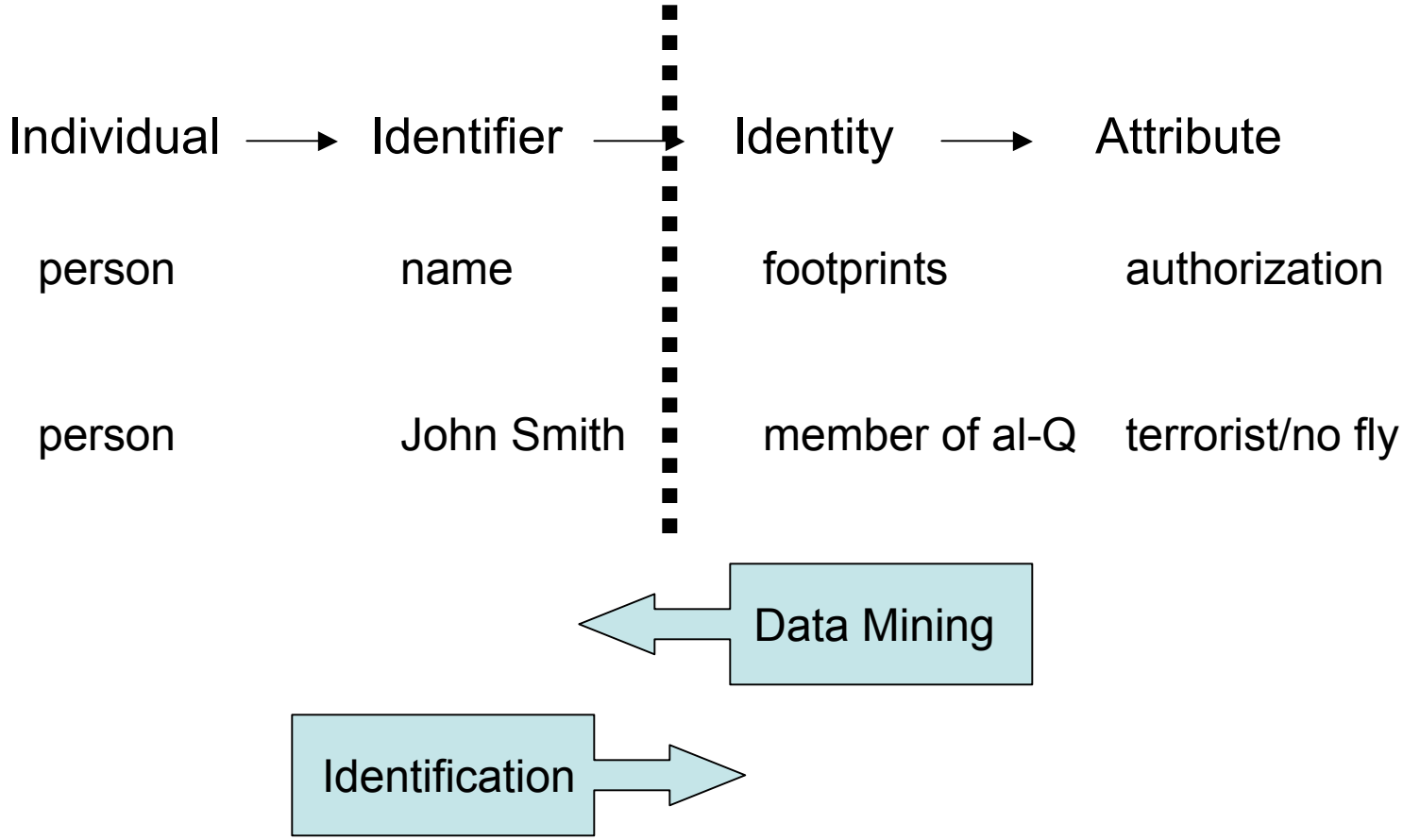
Identification Systems and Domestic Security

Individual →	Identifier →	Identity →	Attribute
person	name	footprints	authorization
person	John Smith	member of al-Q	no fly list

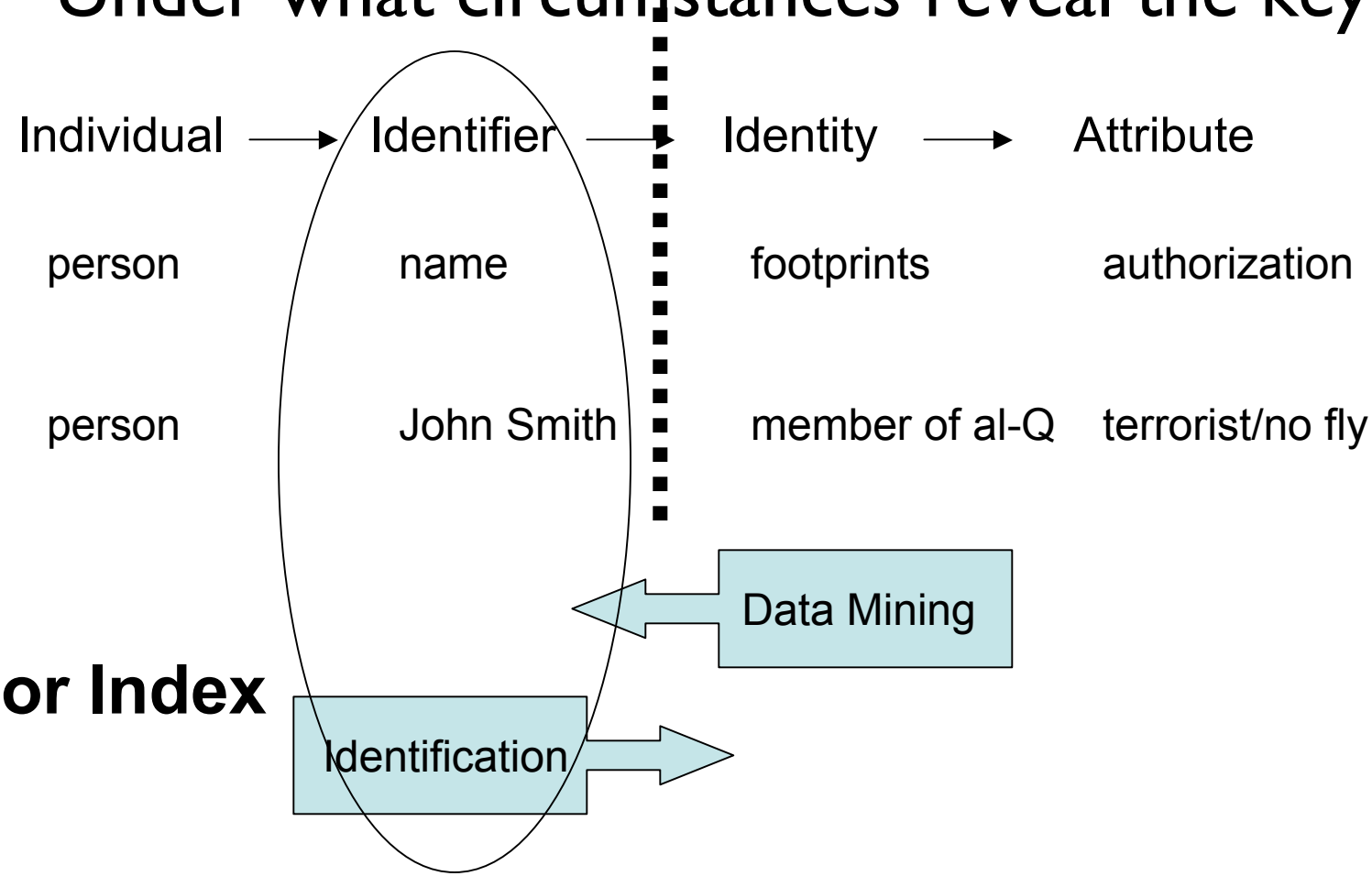
Privacy Divide



Intrusive Technologies



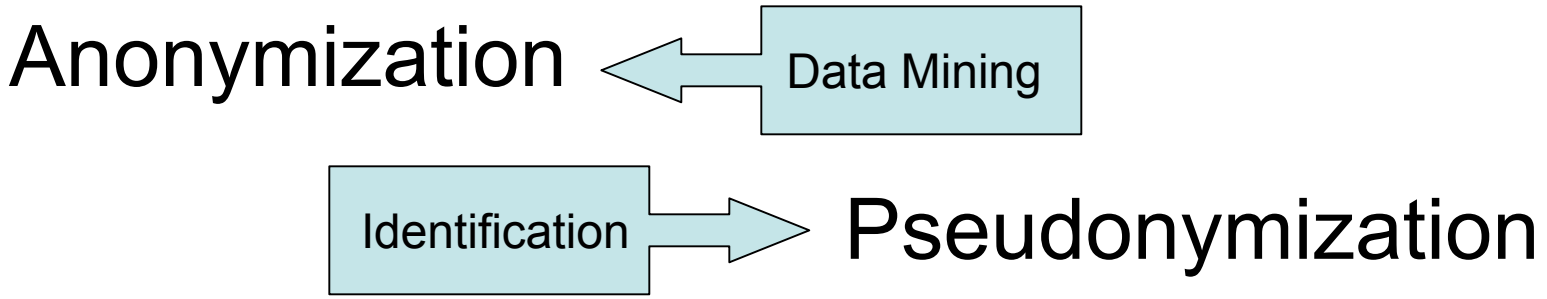
Privacy Policy Question for Identification: Under what circumstances reveal the key?



Key or Index

Potential Technology Solutions

Individual	Identifier	Identity	Attribute
person	name	footprints	authorization
person	John Smith	member of al-Q	terrorist/no fly



Anonymity

- An anonymous record or transaction is one in which the data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data
- Cf., encryption (lock and key) (not truly anonymous) with one-way hash (sausage) (truly anonymous data)
- With one-way hash your data can be turned over to "your worst enemy"

Pseudonymity

- A pseudonymous record or transaction is one that cannot -- in the ordinary course of events -- be associated with a particular individual.
- Form of "traceable anonymity"
- Pseudonymity requires legal, organizational or technical procedures so that the association (that is, the index) can only be accessed under specified circumstances
- Pseudonymity aka "identity escrow"

Value Sensitive Technology Development

- Pyrrhic victory of TIA defunding (whack-a-mole)
- Rather than oppose technology development or outlaw technologies or techniques those concerned with civil liberty protections should become involved in technology development
- Value sensitive design strategies can help build privacy protecting features into technologies and systems

An Example: A "Privacy" ID

- A national ID based on smart card technology
- that only reveals attributes relevant to the particular authentication required to complete the specific transaction
  - Traffic stop -- authorized to drive
  - Commercial transaction -- authorized credit
  - Neither transaction requires transfer of identity
- but, that can still be used for security or law enforcement by allowing one-way hash matching against DB or list
- and, that self-audits -- card logs who queried what when
- Policy question: under what circumstances or predicate particular matches are allowed
- Technology question: how to build those policy rules into the technology and system

Develop System to Protect Privacy

- Anonymize Data
  - Use one-way hashing for data match or data analysis (including data mining) (no initial transfer of raw data)
  - Use SALT and rule-based processing to conform search to policy
- Pseudononymize Identity
  - Develop identification systems that "escrow" identity keys through legal, organizational and technical mechanisms
- Use stringent, transparent procedural mechanisms to control identity resolution through selective revelation

Conclusion

- Security and privacy interests do not present a dichotomous choice between identity and anonymity
- Rather, the question is how to build systems for traceable anonymity (pseudonymity) that support both security and privacy needs
- Pseudonymity can preserve privacy (through anonymity in the ordinary course of events and political autonomy) but also allow for security concerns to be addressed (match watch lists, verify authorization and provide accountability through exchange of digital hashes)
- Assumes legal, organizational and technical mechanisms are devised to protect identity escrow

Challenge

- To discuss, design and implement the legal, organizational and technical mechanisms to allow for pseudonymous social activity
- Thus, insuring freedom in a networked database environment in which all transactions leave electronic footprints