THE CENTER FOR ADVANCED STUDIES
IN SCIENCE AND TECHNOLOGY POLICY

Public Safety versus Personal Privacy: The Case For and Against "Secure Flight"

K. A. TAIPALE
EXECUTIVE DIRECTOR
CENTER FOR ADVANCED STUDIES
SENIOR FELLOW
WORLD POLICY INSTITUTE

PRESENTED AT:
INFO SECURITY 2004
NEW YORK • DECEMBER 8, 2004

Prelude

- Security and privacy (not a balancing act)
  - "Security and privacy are not dichotomous rivals to be traded one for another in a zero-sum game; rather, they are dual obligations of a liberal republic each to be maximized within the constraints imposed by the other"
- Privacy ≠ absolute secrecy (cf. EPIC, EFF)
- Use of advanced information technology (CDT, Markle)
  - Information sharing
  - Data analysis, including data mining
  - But, with appropriate organizational, procedural, and technical safeguards
- Difference is also tactical:
  - opposition (a priori rules) vs. engaged development (iterative)
  - CAS is not opposed to government screening, if done correctly

Obligatory self-promotion

Center for Advanced Studies
www.advancedstudies.org

Technology, Security and Privacy:
The Fear of Frankenstein, the Mythology of Privacy
and the Lessons of King Ludd
7 Yale J. L. & Tech. (Dec. 2004)
Int'l J. Comm. L. &. Pol'y (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

Nevertheless …
the Case against "Secure Flight"

- Dependant on faulty Watch Lists
- Uses problematic "identifiers"
- Lacks effective error correction procedures
- Probably unconstitutional
- Identification systems ≠ security
- Cf. IRTPA §4012 (12/07/04)

Dependant on Faulty Watch Lists

- Watch List "integration" problems
  - Different (incompatible?) criteria
    - "selectee", "no fly", "FBI terrorism watch list", IC/CIA, others
    - FBI memo: "confusion in the field … [on difference between lists]"
  - Diffuse responsibility (no responsible data owner)
    - TTIC (all source integration) --> TSC --> TSA
    - Current TSC-LE procedure for verification is not scalable (ad hoc)
    - Process is used to collect additional data
    - "hits" referred to FBI Counterterrorism watch group
  - Dilution (how useful is non-exclusive list?)
    - 9/11 - 16 names on "no fly" list
    - 12/02 - "thousands" 12/04 - 200K 12/05 - ???
    - Bureaucratic/cya incentive to add names
  - IRTPA 4012(c) (DNI/TSC report on criteria, standards, certainty and threat, consequences w/in 180 days)

Uses problematic “identifiers”

- Non-exclusive identifiers, identities, and attributes
  - Identifiers (in theory)
    - Name, passport #, DOB, country of origin
    - Want to add 14 additional unspecified
  - Identifiers (in reality)
    - Names (including “aliases”) (AIQ info ops)
      - Like names = false positives (Ted Kennedy, David Nelson, etc.)
      - Slight variations = false negatives (Mark Hatfield/TSA quote)
      - IRTPA “authentication” key for false positives
      - what about true positives? (see consequences)
  - PRN problems
    - Travel agent vs. passenger info
    - DOB not included
    - Reveals additional info (type of meal, travel companions, hotel info, etc.)
  - Commercial databases?

Lacks effective error correction procedures

- TSC will not confirm or deny a particular identity
  - How do you find out you are on, and
  - Why (from what sources and on what criteria)
- Ad hoc nature of matching process (II)
  - Current TSC-LE not scalable
  - Airline confirmation process can take hours of involuntary detention (state action? Cf. *Terry* < 1 hour)
- How do you get off? §4012(a)(1)(C)(iii)(I)
  - Referral to TSA "ombudsman" (good luck!) (phone #)
  - Ted Kennedy required three weeks and intervention by Ridge
  - IRTPA "timely and fair process" to appeal and correct

Probably unconstitutional - ID/screening

- Can you be required to present ID to travel?
  - *Gilmore v. Ashcroft* ("other methods of travel") ("SSI" rule)
  - *Hiibel v. Nevada* (compelled ID during *Terry* stop)
  - Fixed and roving checkpoints (border) (Customs)
  - 9/11 implementation (S.2845) -- 'an integrated screening system' which 'shall be designed to encompass an integrated network of screening points that includes the Nation's border security system, transportation system, and critical infrastructure or facilities that the (DHS) secretary determines need to be protected.' (not in IRTPA)
  - How about to enter a mall? Enter a movie? A bar?

Probably unconstitutional - denying access

- Consequences of positive match cf. §4012(c)(2)(D)
  - Gather additional information (ad hoc process)
  - Referred for additional scrutiny
  - Denied access (under what authority?) (true positive)
  - Referred to Law Enforcement
    - "preventative" detention
    - Selective enforcement of collateral "crimes"
    - Deportation
  - Arrest and trial subject to due process
- Fifth Amendment - Due Process

Identification systems ≠ security

- Trusted system problem
  - access v. accountability
  - “not yet untrustworthy”
- Shrinking and porous perimeter
  - InfoSec: Network (firewall), Application (code scanner), Data (resilience)
  - NatSec: Border (Customs, INS, State), “Systems” (TSA, DHS), Individual (seed value of catastrophic outcomes)
  - IRTPA Title IV (transportation) and Title V (borders)
- Identification system ≠ security
  - Knowledge of identity v. knowledge of behavior
  - Cf. CAPPS II

But, if we are going to build identification systems …

- it should encourage pseudonymity
  - Separate knowledge of behavior from knowledge of identity by developing systems based on the anonymization of data (for data sharing, matching and analysis technologies) and the pseudonymization of identity (for identification and collection technologies)
  - Allow social anonymity and autonomy
- be based on a pseudonymous national ID
  - More privacy
  - Same (or better) security

Goal

Security and privacy
not
(false) security and (no) privacy

Caveat

POV 9/11