Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment

National Academies (Herb Lin)

ISPAB Briefing

December 3, 2008

Committee

- Bill Perry, Stanford
- Chuck Vest, MIT/NAE
- Earl Boebert, Sandia
- Michael Brodie, Verizon
- Duncan Brown, JHU
- Fred Cate, Indiana University
- Ruth David, ANSER
- Ruth Davis, Pymatuning Group
- Bill DuMouchel, Lincoln Technologies
- Cynthia Dwork, Microsoft Research
- Steve Fienberg, CMU
- Bob Hermann, Global Technologies
- Gil Kerlikowske, Seattle Police Dept.
- Orin Kerr, GWU Law School
- Bob Levinson, Berkeley
- Tom Mitchell, CMU
- Tara O'Toole, U Pittsburgh
- Daryl Pregibon, Google
- Louise Richardson, Harvard
- Ben Shneiderman, Univ. Maryland
- Danny Weitzner, MIT, W3C

Committee Expertise

- Former Defense Secretary
- Retired Senior Intelligence Official
- Police Chief
- Academic Data Base Experts
- Academic Statistics Expert
- Senior Technology Personnel from Google, Microsoft, and Verizon
- Academic Terrorism Expert
- Academic Bioterrorism Expert
- Experienced Intel and Defense leaders and contractors
- Three Lawyers from across the political spectrum

Task

- Address the challenges of technology for countering terrorists, especially
  - Data mining and information fusion
  - Available and emerging surveillance technologies and their IT support
  - Behavioral surveillance
  - Attendant privacy issues

The Ever-Present Tension?

Protection of our Nation or Privacy and Civil Liberties

Protection of our Nation and Privacy and Civil Liberties

Committee view:

Sometimes “or”, sometimes “and”

Basic Premises

- The United States faces two real and serious threats from terrorists.
  - Terrorist acts themselves, and
  - Inappropriate or disproportionate responses to them.
- The terrorist threat does not justify government activities or operations that contravene existing law.

Basic Premises, cont'd

- Terrorist challenges do not warrant fundamental changes in our level of privacy protection.
- Science and technologies are important dimensions of counterterrorism efforts.
- Counterterrorist programs should provide other benefits when possible.

In short…

- We want the counter-terrorism community to have the best possible tools.
  - With realistic assessment of capabilities and effectiveness.
- We want our privacy protected.
  - Through oversight, assessment, common sense, lawfulness, and continual improvement

The Framework

The Core of the Report

- A **Framework** for Evaluating Information-Based Programs for
  - Effectiveness and
  - Consistency with U.S. Laws and Values
- Applicable to all information-based programs for specific government purposes, such as counterterrorism, both classified and unclassified.

The Committee believes this framework:

- Is realistic;
- Broadly applicable;
- Consistent with U.S. laws and values;
- Based on common sense, best practice, and lessons learned; and
- Leads to continuous improvement and accountability.

Framework: Effectiveness

Programs should have or be:

1. Clearly stated purpose-what are you trying to achieve
2. Rational Basis—why should we even think it might work?
3. Sound Experimental Basis—is there empirical demonstration that it can work?
4. Scalable—will it work at scale?
5. Operations or Business Processes—how does the program work within itself?
6. Capable of being integrated with other inter- and intra-organizational entities—how does it interact with other elements?

Framework: Effectiveness

Programs must have or be:

7. Robust-is it resistant to countermeasures?
8. Appropriate and Reliable Data—is the data good?
9. Data Stewardship-is the data protected properly?
10. Objectivity-who evaluates the program? (not program advocates!)
11. Ongoing Assessment—programs evolve, and evolved version requires examination as well
12. Documented—are effectiveness and compliance documented? Or merely asserted?

Framework: Consistent with U.S. Laws and Values

1. **Data**
   - Need—why is personal data needed?
   - Sources—where does data come from? Is it legal?
   - Appropriateness—are data good for the intended use?
   - Third-Party Data require additional protections
     - Repurposed data should be explicitly repurposed
     - Leave 3rd party data in place if possible
     - Consider adequacy explicitly

Framework: Consistent with U.S. Laws and Values

2. Programs

- Objective of program - clear and lawful?
- Compliance with existing law?
- Effectiveness – scientifically demonstrated to be effective?
- Frequency of false positives – acceptable?
- Reporting and redress of false positives – how to report? How to correct?
- Impact on individuals – what happens to individuals?
- Data minimization – are data in excess of what is necessary collected?
- Audit Trail – can users of the data be held individually accountable for abuse or non-compliance?
- Security and access – are unauthorized users kept out?
- Transparency – are the impacts and operation of the program understood by those affected by it?

Framework: Consistent with U.S. Laws and Values

3. Administration and Oversight

- Training – are users properly trained to use the program?
- Agency Authorization – is the program actually authorized by the agency?
- External Authorization – are mechanisms for obtaining external authorization in place when necessary?
- Auditing for Compliance – is compliance reviewed at least annually?
- Privacy Officer – is a policy-level officer in place to manage privacy issues?
- Reporting – are all relevant policy makers kept informed and up to date about program operation?

Conclusions

Conclusions: Privacy

- Privacy protection can be obtained through the use of a mix of technical and procedural mechanisms.
- Data quality is a major issue in the protection of privacy.
- Inferences about intent and/or state of mind implicate privacy issues to a much greater degree than assessments or determinations of capability.

Conclusions: Assessment of Counterterrorism Programs

- Program deployment and use must be based on criteria more demanding than “it’s better than doing nothing.”

Conclusions: Data Mining

- Currently, privacy violations arising from information-based programs using data mining and record linkage are not adequately addressed.

- Data mining has been successful in private sector applications such as fraud detection. However, detecting and preempting terror attacks is vastly more difficult.

Conclusions: Data Mining, Cont'd

- Pattern-based data mining can help analysts determine how to deploy scarce investigative resources and actions. Automated terrorist identification is not feasible.

Conclusions: Data Mining, Cont'd

- Systems that support analysts should have features that enhance privacy protection; however, privacy-preserving examination of individually identifiable records is not possible.
- Data mining R&D using real population data is inherently privacy-invasive.

Conclusions: Deception Detection and Behavioral Surveillance

- Behavioral and physiological monitoring techniques might help detect: (a) individuals whose behavior and physiological states deviate from norms and (b) patterns of activity with well-established links to underlying psychological states.

- R&D aimed at automated, remote, and rapid assessment of anomalous behavioral and activity with well-established links to psychological states relevant to terrorist intent is warranted.

Conclusions: Deception Detection and Behavioral Surveillance

- Technologies and techniques for behavioral observation have enormous potential for violating privacy.

We also say-

- “neither the relevant scientific community nor this committee has reached a consensus on whether any behavioral surveillance or physiological monitoring techniques are ready for use today for counterterrorism given the present state of the science.”

Conclusions: Statistical Agencies

- Federal census and survey data has little or no content that would be useful for individual tactically oriented counter-terrorist activities, because of their content, sampling fractions, and lack of personal identifiers.

Recommendations

Recommendation 1

Government agencies using information-based programs for counter-terrorist purposes should follow a systematic process such as the one described in the committee's framework to evaluate the desirability and feasibility of any given program before such a program is set into motion.

Sub-Recommendations specify:

- Periodic application of Framework after deployment
- Use of synthetic population data for R&D
- Robust, independent oversight of programs and
- Redress for innocent individuals harmed by programs.

Recommendation 2

The U.S. government should periodically review the nation's law, policy, and procedures that protect the private information of individuals in light of changing technologies and circumstances. In particular, the U.S. Congress should re-examine existing law to consider how privacy should be protected in the context of information-based programs (e.g., data mining) for counterterrorist purposes.

For more information contact:

Herb Lin

202—334-3191

hlin@nas.edu