Woodrow Wilson International Center for Scholars
Foresight and Governance Project

OPEN DIALOGUE
ENHANCING NATIONAL SECURITY AND CIVIL LIBERTIES IN THE INFORMATION AGE

The **Headlines** from a Meeting at the Woodrow Wilson International Center for Scholars May 22, 2003

"Opinions are formed in a process of open discussion and public debate, and where no opportunity for the forming of opinions exists, there may be moods – moods of the masses and moods of individuals, the latter no less fickle and unreliable than the former – but no opinion."

-- Hannah Arendt, On Revolution, 1963

Background

The events of September 11th made explicit the effectiveness of asymmetric operations such as terrorism against our country. We know that the democracy and freedom we all take for granted imply many vulnerabilities to asymmetric attacks. America has always responded to such challenges with technology. So can technology help us preserve our freedoms while mitigating these vulnerabilities? Can technical tools that facilitate collection, analysis, and dissemination of information throughout the first-responder, law enforcement, intelligence, and military sectors help ensure homeland security? Numerous research and acquisition programs have been initiated in the last 18 months to evaluate and field test such systems. But by their very nature these programs have run into privacy issues, many of them jurisdictional firewalls that are decades old.

Recent examples of such controversial programs include DARPA's Terrorism Information Awareness (TIA) project and TSA's Computer Assisted Passenger Pre-screening System (CAPPS II). Many concerns have been publicly voiced about the proper balance between privacy protection and national security that these programs entail. While a dialogue on such new capabilities is essential, the picture thus far has often been clouded and shaped more by emotion than reality. The highly politicized nature of the debate has precluded a dispassionate discourse about the merits and risks associated with such technologies. The end result may be the loss of a whole genre of valuable technical tools -- tools that could prevent future terrorist attacks. The Foresight and Governance Project at the Woodrow Wilson International Center for Scholars is hosting an open dialogue and forum to examine the balance between civil liberties and national security in an effort to find ways of breaking this vicious cycle.

The main goals were to:

- Inform the debate by presenting an accurate view of the technologies being developed.

- Define the landscape of policy issues which such technologies raise, and the implications for our civil liberties.

- Discuss perspectives on how to strike the right balance between the social costs and benefits of these technologies.

- Develop a better understanding of the dynamics of the public debate surrounding such issues.

Presentations/Comments were made by the following people:

- **John J. Hamre**, President and CEO, Center for Strategic & International Studies
- **Robert Popp**, Deputy Director, DARPA / Information Awareness Office
- **Paul Rosenzweig**, Senior Legal Research Fellow, Heritage Foundation
- **Jim Dempsey**, Director, Center for Democracy and Technology
- **Stuart Taylor**, The National Journal
- **Heather Mac Donald**, Manhattan Institute
- **Christopher Ford**, State Department

Region/State

Evening Herald

Are scientists afraid of Ed Conrad?

THE HEADLINES

- There is a large difference between reality and public perception concerning DAPRA's Terrorism Information Awareness (TIA) Program, some of this being driven by unrealistic and uninformed portrayals in the media.

- There is a tendency to see the DARPA technology development work as existing or inevitable. DARPA funds very high risk, high payoff, research, so the technologies being proposed or developed under the TIA program may not be deployed for years, or at all.

- The research portfolio of TIA contains technologies that do not have implications for information policies such as privacy protection (e.g., better peer-to-peer collaboration technologies to help agencies communicate with each other virtually; or foreign language translation technologies to exploit the wealth of information in foreign speech and text).

- The ground rules and legal/policy frameworks for privacy protection are outdated. These rules were designed for a paper-based economy or centralized databases and not readily applicable to today's intelligence challenges and emerging information technologies allowing for a more interconnected society.

- Existing privacy safeguards (many relying on “fair information practices” and social contract) on the civil side may be ineffective when data is transferred to the government side for intelligence purposes. The proposed TIA technologies need to be built consistent with principles such as:

  - notice
  - limitation (no more information accessed or analyzed than needed)
  - reuse (data analyzed for one use should not be passed on for another)
  - retention
  - access (I can see the data you have on me)
  - redress (I can correct errors in that data).

  Redress and access are key issues that must be solved. However, some of these principles may not be readily transferable to the intelligence/law enforcement regime, in which case adequate substitutes must be found.

- Unlike subject-based queries, there is a lack of a policy framework or set of legal protocols to deal with the type of pattern-based queries being tested or contemplated under the TIA program. A model analogous to “probable cause” coupled with a privacy protection approach such as “selective revelation” appears to be a reasonable starting point to justify such searches.

- Both the creators and the <u>users</u> of technologies such as those being developed in TIA must be sensitized to civil liberties issues (training may be necessary).

- Safeguards should be “hardwired” into these technologies whenever possible, including tamper-proof audit trails, policy and business rule enforcement, encryption, etc.

- The problem of false positives is a challenge and concern – both technically and from a policy perspective – for any predictive system such as TIA and will need to be contended with.

- DARPA, and other developers of such systems, need to be open and forthright about the technologies under development and their capabilities in order to inform public debate.

- When confronted with these types of technologies, the press will have tendencies to imagine the worse, sanctify the status quo, leave out balancing opinions, and not explore alternative solutions (as well as their costs and benefits).

- Assume technological and scientific illiteracy on the part of the media. Even the best and most well-intentioned reporters will have problems understanding these technologies. DARPA cannot change the press; DARPA must change its strategies for dealing with the press. In attempting to inform the press or public, use examples of what the technologies do, if possible.

- Privacy is a misunderstood concept and makes discussions more difficult. It may be better to focus on anonymity and people’s “expectations” about anonymity.

The dialogue was moderated by Dave Rejeski, Director of the Foresight and Governance Project at the Wilson Center. The event was organized by Victoria Stavridou, SRI International, and Jim Kadtke, Office of Senator John Warner.

About the Woodrow Wilson Center:

The Woodrow Wilson International Center for Scholars is the living, national memorial to President Wilson established by Congress in 1968 and headquartered in Washington, D.C. It is a nonpartisan institution, supported by public and private funds, engaged in the study of national and world affairs. The Wilson Center establishes and maintains a neutral forum for free, open, and informed dialogue. The Center commemorates the ideals and concerns of Woodrow Wilson by: providing a link between the world of ideas and the world of policy; and fostering research, study, discussion, and collaboration among a full spectrum of individuals concerned with policy and scholarship in national and world affairs.