

## Overview

This is the second report of an extraordinary task force we have been privileged to co-chair. This remarkable and diverse group has come together to serve our nation by doing the hard work of considering how we can create an information network that prevents terrorism and protects the security of our homeland, while preserving the civil liberties that are a fundamental part of our national values.

In the Task Force's first report, we stressed the importance of creating a decentralized network of information-sharing and analysis to address the challenge of homeland security. We emphasized the need to form that network around presidential guidelines shaped by public debate on how to both achieve security and maintain liberty. We also set forth principles for capitalizing on our society's strengths in information technology. In this second report, we reaffirm those principles and provide greater detail on how to implement our approach.

The network we envision would be created with the following key elements, which reflect the character of the distributed, asymmetric threat we confront:

1. The handling of information should be decentralized, and should take place directly among users, according to a network model rather than a mainframe or hub-and-spoke model.
2. The network should be guided by policy principles that simultaneously empower and constrain government officials by making it clear what is permissible and what is prohibited.
3. Our government's strategy should focus on prevention.
4. The distinguishing line between domestic and foreign threats is increasingly difficult to sustain. Thus, in its approach, our government should avoid creating blind spots, or gaps between agencies, that arise from this distinction. At the same time, though, our government needs urgently to define new rules—rules to replace the old “line at the border” between domestic and foreign authorities for information-collection and use—to

ensure that agencies do not infringe on our traditional civil liberties.

5. The network should reflect the fact that many key participants are not in the federal government, but rather in state or local government and the private sector.
6. The network should make it possible for the government to effectively utilize not only information gathered through clandestine intelligence activities and law enforcement investigations, but also appropriate information held by private companies. This should happen only after clear articulation by the government of the need for this information and the issuance of guidelines for its collection and use.
7. Combating terrorism is a long-term effort that is designed to protect our way of life and our values along with our security. Therefore, the policies and actions undertaken need to have the support—and trust—of the American people. Privacy and other civil liberties must be protected.

What do these principles mean in practice?

First, our government should give greater priority to sharing and analyzing information. In the Cold War intelligence architecture, the government placed a premium on the security of information. It developed a system that tightly controlled access to information by requiring that every individual have a demonstrable “need to know” certain information before he could see it and by allowing the agency that initially acquired the intelligence to restrict further dissemination of that intelligence. This system assumed that it was possible to determine *a priori* who needed to know particular information. And it reflected the judgment that the risk of inadvertent or malicious disclosure was greater than the benefit of wider information-sharing.

This architecture and the underlying assumptions are ill suited to today's challenges. The events of September 11, 2001, have starkly demonstrated the dangers associated

with the failure to share information, not only within the federal government, but also between the federal government, on the one hand, and state and local governments and the private sector on the other. Therefore, the government should open up the system to state and local agencies and officials and, in some circumstances, to private sector actors, providing access not just to information but to technology and money as well. Our government should reengineer operational processes where needed and build the technology architecture and tools that will facilitate two-way sharing and interoperability. Our government should also take into account the needs of the users, as well as the agency that originally developed the information, in deciding whether or how to control where the information goes. This should take place in an environment in which the need to protect both the security of sensitive information and individual civil liberties is consistently addressed.

Furthermore, our government should effectively utilize the valuable information that is held in private hands, but only within a system of rules and guidelines designed to protect civil liberties. Our nation can never hope to harden all potential targets against terrorist attack. Therefore, we must rely on information to try to detect, prevent, and respond to attacks. The travel, hotel, financial, immigration, health, or educational records of a person suspected by our government of planning terrorism may hold information that is vital to unveiling both his activities and the identities and activities of other terrorists.

But until the government devises consistent guidelines for controlling when and how such information is accessed and used—and until those guidelines are publicly debated—the public’s concerns over potential privacy infringements will continue to hamper the necessary development of new technologies and new operational programs to use that information.

The need to create the network we envision is more urgent than ever. Terrorism remains a continuing threat around the world. And the potential for terrorists to use weapons of mass destruction raises the stakes considerably. Building the technical architecture, changing agency cultures, establishing new rules and procedures, and securing the necessary funding all take time. It is therefore imperative that the steps we recommend receive immediate attention. We urge the Executive Branch and Congress to implement the measures necessary to create the proposed Systemwide Homeland Analysis and Response Exchange (SHARE) Network—which would empower all participants to be full and active partners in protecting our security, and which would be governed by guidelines designed to protect our liberties.

Zoë Baird

James Barksdale

# MARKLE FOUNDATION

## TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE

### *Chairmen*

**Zoë Baird**  
Markle Foundation

**James L. Barksdale**  
The Barksdale Group

### *Executive Director*

**Michael A. Vatis**  
Markle Foundation

### *Members*

**T. Alexander Aleinikoff**  
Georgetown University Law Center

**Robert D. Atkinson**  
Progressive Policy Institute

**Stewart Baker**  
Steptoe & Johnson

**Eric Benhamou**  
3Com Corporation

**Jerry Berman**  
Center for Democracy and Technology

**Robert M. Bryant**  
National Insurance Crime Bureau

**Ashton B. Carter**  
Harvard University

**Wesley K. Clark**  
Wesley K. Clark & Associates

**G. Wayne Clough**  
Georgia Institute of Technology

**William P. Crowell**  
Security and Intelligence Systems

**Sidney D. Drell**  
Stanford University

**Esther Dyson**  
EDventure Holdings

**Amitai Etzioni**  
The George Washington University

**David J. Farber**  
Carnegie Mellon University

**John Gage**  
Sun Microsystems, Inc.

**Slade Gorton**  
Preston, Gates & Ellis

**Morton H. Halperin**  
Open Society Institute

**Margaret A. Hamburg**  
Nuclear Threat Initiative

**John J. Hamre**  
Center for Strategic and International  
Studies

**Eric H. Holder, Jr.**  
Covington & Burling

**Arnold Kanter**  
The Scowcroft Group

**Michael O. Leavitt**  
Governor of Utah

**Tara Lemmey**  
Project LENS

**Gilman Louie**  
In-Q-Tel

**Judith A. Miller**  
Williams & Connolly

**James H. Morris**  
Carnegie Mellon University

**Craig Mundie**  
Microsoft

**Jeffrey H. Smith**  
Arnold & Porter

**Abraham D. Sofaer**  
Stanford University

**James B. Steinberg**  
The Brookings Institution

**Paul Schott Stevens**  
Dechert LLP

**Rick White**  
TechNet

**Philip Zelikow**  
Miller Center of Public Affairs  
University of Virginia

*Participating Experts  
(non-government)*

**Bruce Berkowitz**  
RAND

**Robert Clerman**  
Mitretek Systems

**James Dempsey**  
Center for Democracy and Technology

**Mary DeRosa**  
Center for Strategic and International  
Studies

**Lara Flint**  
Center for Democracy and Technology

**Lauren Hall**  
Microsoft

**Jeff Jonas**  
Systems Research & Development

**James Lewis**  
Center for Strategic and International  
Studies

**Terrill D. Maynard**  
Consultant

**Mary McCarthy**  
Center for Strategic and International  
Studies

**Patrick J. Sullivan, Jr.**  
Cherry Creek Schools

**Winston Wiley**  
Booz Allen Hamilton

### *Associate Director*

**Mary McKinley**  
Markle Foundation

### *Task Force Staff*

**Nancy Boursiquot**  
Administrative Assistant

**Todd Glass**  
Director, Public Affairs

**Caroline McCarus**  
Assistant to the President

**Jennifer Obriski**  
Administrative Assistant

**Stefaan Verhulst**  
Chief of Research

## Acknowledgments

The Task Force issued its first report in October 2002. This initial report was seen as a useful contribution by a broad cross section of those concerned with the new environment for America's homeland security. We decided to continue our work and developed an agenda for further action. The Task Force began its second year in March 2003. Renewing its commitment to providing the government with practical recommendations informed by diverse perspectives, the Task Force organized several areas of work, leading up to a summer plenary meeting. At that meeting, Task Force members agreed that we should issue a second report by the end of this year, given the urgent need for our government to improve its ability to use information to protect our nation.

We organized two Working Groups. Working Group I, ably led by Tara Lemmey and Bill Crowell, focused on how to construct a network for sharing and analyzing information among governmental entities at all levels and relevant private sector organizations. This Working Group's paper is included in Part Two of our report. Working Group II, equally ably led by Gilman Louie and Jim Steinberg, addressed the issue of how our government can more effectively utilize privately held data while protecting privacy and other civil liberties. This Working Group's paper, too, is in Part Two. We also convened a smaller subgroup, thoughtfully led by Amitai Etzioni, to consider the crosscutting issue of how to make forms of identification more reliable while protecting civil liberties. This paper is in Part Three.

The papers developed by the Working Groups and the subgroup, along with many other papers, including the selection of appendices found in Part Three, informed the Task Force's discussions, which took place in two plenary sessions, numerous meetings, and email and telephone exchanges. These discussions led to the Report of the Task Force as a whole, found in Part One.

We thank the leaders of the Working Groups and the subgroup for their devotion to our work and their high standards regarding what we together could achieve. On technology issues, Tara Lemmey, Gilman Louie, and Task Force associate Jeff Jonas made our work a central part of their daily lives, tirelessly researching and vetting papers,

drafting sections of our report, and informing our efforts with their knowledge and creativity. On policy and governmental issues, Jim Steinberg, Amitai Etzioni, Stewart Baker, and Task Force associates Mary DeRosa, Mary McCarthy, Winston Wiley, Terry Maynard, and Jim Dempsey developed innovative approaches, careful research, compelling ideas, and drafts of sections of the report. These people and the many other members and associates of the Task Force put in dozens of hours melding their expertise into a common understanding of the interplay between technology and policy. They attended meetings, reviewed documents, consulted one another via email or telephone, and sought advice and information from other professionals. We cannot adequately thank them here for their wisdom and dedication.

Eric Benhamou, among his other contributions, helped us chair our principal plenary meeting. Lauren Hall and a team at Microsoft—drawn together by Task Force member Craig Mundie—assisted Tara Lemmey in helping us think through how to create visual representations of our recommendations.

Stefaan Verhulst, Lara Flint, and Tanvi Madan provided valuable research assistance. Todd Glass handled our public education and outreach, and Karen Thomas provided an excellent platform on the Internet for the Task Force's work. Sharon Lucius and Caroline McCarus were important members of the team, as were Paulette Layton, Nancy Boursiquot, Jennifer Obriski, Brendan Lavy, and Linda Hutchins, who worked day to day to support the Task Force members and staff. Karen Byers provided sound financial management. Mila Drumke tirelessly edited our final product.

Finally, none of this would have been possible without the dedication and hard work of our Executive Director, Michael Vatis, and Associate Director, Mary McKinley. Michael thoughtfully managed the many different areas of activity that constituted this project and ultimately brought them together to form a valuable whole in this report. Mary again operated the daily activities, keeping them on course with professionalism and experience.

Zoë Baird

James Barksdale