

**We Cannot Fight Terrorism Without Better Information**  
by Zoë Baird and James Barksdale

Today, our government does not have the information it needs to fight terrorism. And the pieces of information it does have are still isolated in different agencies and therefore we cannot see their significance. Discussion over the 9/11 Commission's recommendations to establish a National Intelligence Director and a National Counterterrorism Center are important to fix this and other problems. Another recommendation has gotten less attention and can be implemented immediately by the President to serve any organizational structure. A critical first step in getting us the information we need is to create a "trusted information network" to facilitate better information sharing among our intelligence agencies. This recommendation has broad nonpartisan support and if undertaken now it can make America safer immediately.

Information is key to fighting terrorism and enhancing our security. By adopting technologies used in the private sector everyday, the government can set up a network that substantially improves our agencies' ability to share information in order to prevent terrorist attacks. With a Presidential directive, our intelligence agencies could start the flow of valuable information immediately. For example, electronic directories could be quickly created to link all the analysts in different agencies working on the same problem, identify experts in the private sector and universities, and indicate which agencies have information on subjects of interests. These actions do not need to wait until we have all the steps in place to begin sharing the text of the documents themselves.

The 9/11 Commission embraced the recommendations for creation of a Systemwide Homeland Analysis and Resource Exchange (SHARE) Network made last December by the Markle Foundation Task Force on National Security in the Information Age, which consists of leading national security experts from the Carter, Reagan, Bush and Clinton administrations, as well as widely recognized experts on technology and civil liberties.

The SHARE Network represents a "virtual reorganization" of government by fundamentally altering how information is used to facilitate better, faster decision-making at all levels of government. And when paired with clear guidelines to govern the system and effective oversight, the use of information technology can also be the best way to protect privacy and civil liberties.

Say a field agent at the Chicago FBI office and a CIA operative in Kabul become aware of separate leads that if put together might point to a bio-warfare attack in Chicago. Under the current system, reports from these two agents are unlikely to be put together or raise any red flags. However, using the SHARE Network, these reports would be linked through similar key words such as "virus" and "Chicago" or other linking tools. Instead of being housed in classified files at the CIA and FBI, these reports would be distributed electronically to people who should see them. They also would be posted and available to be pulled by network participants with a particular interest. An analyst at Terrorist Threat Integration Center (TTIC), for example, might see both reports, contact the CIA

and FBI agents and others to discuss their reports, begin to connect the dots and define actionable objectives.

The FBI, CIA, and TTIC players could form ad hoc task forces of people with common interest and reach out to other relevant agencies and individuals for more information. And they could organize the work themselves, without losing time or going to their superiors in Washington for approval.

Based upon their discussions, this group could now create actionable intelligence for their agencies. The CIA might elevate the information to a higher level, to the director, or perhaps up to the President. Through local contacts, the FBI could notify local police to watch for activities related to a potential plot.

The SHARE Network protects privacy and civil liberties by emphasizing use of anonymous data until an individual's identity is required, by restricting access to certain kinds of personally identifiable information, and by using systems to verify the identities of those permitted access. In addition, guidelines governing the system would both empower and constraint the participants involved.

Some government agencies have begun using key elements of the SHARE Network. However, for this networked approach to succeed, an agency-by-agency approach is inadequate. What is needed is a national framework, guided by both the President and Congress. Senators Lieberman and Collins, with others, have already introduced bipartisan legislation to create a SHARE Network. The Markle Task Force has called on the President to issue a directive that would set the goal for creating the SHARE Network and include clear government-wide policy guidelines for the government's collection and use of domestic information, including private sector information about U.S. persons. By doing so, the President would provide the leadership necessary to overcome the systemic barriers to information sharing, which seriously hampered the efforts of our nation's intelligence agencies prior to the September 2001 terrorist attacks, and unfortunately still exist today.

Information-sharing itself is not the goal; rather, it is the means by which we can effectively enhance security and protect privacy, by maximizing our ability to make sense of all available information. To accomplish this, we must shed our current 'need to know' Cold War mentality and replace it with a culture based on the 'need to share.' Such an approach would substantially and immediately improve our ability to predict and prevent terrorist attacks. The technology exists to build such a network; what's needed now is the leadership to get the information flowing.

*Zoë Baird, President of the Markle Foundation, and James Barksdale, CEO of Barksdale Management Inc. and former CEO of Netscape, are co-chairs of the Markle Foundation Task Force on National Security in the Information Age.*