

Enhancing Security and Civil Liberties
An open letter from Dave Farber, Esther Dyson and Tara Lemmey
October 6, 2004

As long-time civil liberty and privacy advocates, we are concerned with any government program or new technology that could lead to a loss of the personal freedoms that all Americans have a right to. Thus, as we consider how technology can help our government more efficiently fight the war on terror, we are also looking for ways that it can enhance rather than constrain those rights, most particularly in limiting the dissemination of information that is not relevant to an investigation, and in supporting more monitoring and accountability in the use of data by government agents.

For the past three years, we have brought this perspective to the Markle Foundation Task Force on National Security in the Information Age, a group that has dedicated considerable time and resources to determine how best to mobilize information to improve security while protecting established liberties. Legislation currently being debated in Congress to implement the 9/11 Commission recommendations to reform our nation's intelligence community includes a provision based largely on the Task Force's work calling for the creation of a trusted information network that would foster better and more targeted information sharing and substantially improve our ability to predict and prevent terrorist attacks while at the same time meeting our goals for protection of civil liberties.

The Markle Task Force consists of leading national security experts from five administrations, as well as widely recognized experts on technology and civil liberties. Over the last several years, the Task Force's work has broken new ground on how technology and policy can be used together to enhance security and privacy. The Task Force's latest report, *Creating a Trusted Information Network for Homeland Security*, details the necessary elements of a proposed System-wide Homeland Analysis and Resource Exchange (SHARE) network that would more effectively combat terrorism than does our current system, while protecting privacy.

If our recommendations are adopted - as looks likely - it is vital that they be adopted completely, with the important protections for civil liberties implemented thoroughly and in good faith. Lip service is not enough.

The SHARE network would allow us to move from our current Cold War mentality of classification and "need to know" to a system better able to counter the threat of terrorism. This new approach is based on the idea of the "need to share" and is governed by clear government-wide guidelines on how information is collected and used and by whom, as well as strong oversight provisions built into the design of the network.

During the course of the debate in Congress over the implementation of the 9/11 Commission recommendations, valid questions have been raised over civil liberty

concerns and role of such an information sharing network. We grappled with these same questions as we worked through our recommendations for the Task Force. We also learned important lessons from the problems of other efforts like the Total Information Awareness program (TIA) and MATRIX, both of which have raised serious privacy concerns. We eventually determined that you can achieve a balance between security and privacy if you ensure that strong guidelines, transparency, accountability and oversight are built into the network from the start.

In addition to the approach of building policy into the design of the network, the Task Force also designed the network not as a centralized database, but as a set of pointers and directories that allow only authorized users to gain access to information. The system also calls for regular and robust internal audits of how information is collected and stored and used. Privacy technologies such as anonymization, permission controls, and audit trails are built into the design of the network to prevent abuse. In addition, the Task Force also calls for a phased implementation to allow for appropriate public comment and a strong civil liberties board to oversee the system and ensure that privacy

The SHARE network capability, if implemented properly, would give us the ability to overcome the systematic barriers to information sharing that so seriously constrained our intelligence agencies prior to the 9/11 terrorist attacks, and that unfortunately still exist today. It would also provide us with the best opportunity not only to balance security and privacy, but to enhance them both as well.

David Farber is Distinguished Career Professor of Computer Science and Public Policy at the School of Computer Science at Carnegie Mellon University. He also serves on the Board of Trustees of the Electronic Frontier Foundation. Esther Dyson is editor at large, CNET Networks and former chairman on EDventure Holdings, recently sold to CNET. She also served as founding chairman of the Internet Corporation for Assigned Names and Numbers from 1998 – 2000. Tara Lemmey is founder and CEO of LENS Ventures Inc., a network of experts focused on innovation in technology, science, law and economics. She previously served as president of the Electronic Frontier Foundation. They are all members of the Markle Foundation Task Force on National Security in the Information Age. For more information on the Markle Foundation Task Force on National Security in the Information age, please see www.markle.org.