

**Building Trusted Information-Sharing Environments for National
Security and Health Care**

Key Note Speech

Web-Enabled Government: Transforming the Business of Government
The e-Gov Institute

June 1st, 2005

By Zoë Baird
President, Markle Foundation

INTRODUCTION

Good afternoon. It is a pleasure to be here today with colleagues both in the government and from other sectors to discuss how we can best transform the business of government through sharing information and using information technology (IT). I thank the e-Gov institute for the privilege of participating in today's meeting.

There are few matters more important to the future of our government and American society than the challenge we are grappling with here today. Advances in information technology continue to promise a future with possibilities that go far beyond the revolutionary change we have already witnessed in business, finance, and consumer choice. In fact, I'm sure that all of us here today share the belief that technology, woven into the fabric of institutions serving the public, can re-engineer how information is used to meet critical public needs, and empower people to improve their lives.

Aware of the transformative potential of IT, the Markle Foundation has worked for the last few years on the creation of trusted information-sharing environments in both national security and health care. We have been working with many collaborators from government and the private sector to achieve two major goals:

- **The first goal is to strengthen our nation's security while protecting civil liberties.**
- **The second goal is to modernize our complex and over-burdened healthcare system while preserving personal privacy.**

These are two of the most critical challenges of our time, in which it is clear that the benefit of putting the right information in the right hands at the right time is enormous. In each of these areas, we know that the effective and appropriate use of IT can literally save lives. We also know that our nation's goals in both areas cannot be met without better use of IT.

At the same time, national security and health care also put into sharp focus a critical challenge: protecting our established civil liberties and personal privacy as we seek new ways to transform our lives through information and information technology. This must be done from the outset, not as an afterthought. Policies and business rules must be in place at the moment the sharing of sensitive information occurs. Otherwise, public trust may be undermined and this may weaken our ability to implement the exchange of information. Clearly, the policies and rules for these efforts must be developed in a transparent, inclusive, and accountable manner in order to allow for legitimate outcomes.

In the National Security environment, we created the Task Force on National Security in the Information Age, a distinguished panel of security experts from five administrations, as well as experts on technology and civil liberties, which I am

privileged to co-chair with Jim Barksdale. In health care, we support and manage Connecting for Health, a public-private collaborative consisting of an extraordinary group of government, industry, technology, consumer, and healthcare leaders, which has championed electronic connectivity in the national health care debate.

I was asked by the organizers of today's e-Gov Conference to reflect on the challenges in implementing an information-sharing environment. In a few minutes, I will focus most of my remarks on implementation of the information-sharing environment in the Intelligence Reform Act.

Yet, before I do so, I am delighted to note that earlier today our Connecting for Health initiative announced a new and very significant effort, which will undoubtedly make significant progress toward developing a nation-wide health information exchange or health information-sharing environment.

LAUNCH OF A PROTOTYPE

Today, Connecting for Health announced that it is launching a prototype for a nationwide health information exchange.

This effort is one of the first steps toward achieving the transformative vision I'm sure we all share -- enabling patients and authorized physicians anywhere in the U.S. to share important, even life-saving, personal health information on a completely voluntary basis in a secure and private manner.

Managed by the Markle Foundation and funded by the Markle Foundation and one of our partners, the Robert Wood Johnson Foundation, this new initiative will allow authorized users of three very different health information networks located in California, Massachusetts, and Indiana to share health information across state lines with each other.

These three local communities share a commitment to empowering patients to take an active part in their health care, increasing the quality of medical care, reducing costs, protecting personal privacy, and encouraging local autonomy and innovation in electronic communication. By adopting common technology standards for describing and sending health information, these efforts will also demonstrate national interoperability between regional networks.

We are launching this prototype at a unique moment in time. Last year, the President issued an Executive Order and a Report on Innovation, calling for every American to have an electronic health record within the next ten years. In addition, HHS has established the National Health Information Technology Coordinator and is currently considering how to create a national health information-sharing environment. We believe that the lessons learned through the Connecting for Health initiative will contribute to efforts by the government and others to establish a policy and technical framework that reflects public values.

This new effort will inform government, consumers, and the private sector about immediate steps to achieve improvements in health care quality and efficiency through information sharing and information technology.

Its key elements are:

- patients and their authorized health professionals jointly make decisions regarding the sharing of health information;
- Information about patients is stored in the electronic files of the health professionals and institutions responsible for patient care and with the patients own record, and not in one central national database;
- a nationwide health information exchange is created on the Internet, not as a completely new network;

- communication among numerous, disparate information networks and diverse communities is facilitated; and
- there is diversity in software and hardware in the system.

It is critical, as we approach information sharing in health care, that we not make the same mistakes the government made with national security projects like the FBI's Virtual Case File or DARPA's Total Information Awareness—where the policy goals and constraints were not clearly defined so they could drive the technology development.

MARKLE TASK FORCE

These principles for transforming health care share much in common with the principles recommended by the Markle Task Force on National Security in the Information Age for increasing national security, while protecting established civil liberties. The networked environment we are working to establish would bring together disparate data to help the government draw a meaningful picture of potential terrorist threats. At the same, it would assure that established civil liberties are protected. Just as in health care, we are committed to having our Nation's common values shape the technological solutions we pursue.

In that spirit, the Markle Task Force on National Security recommended the development of a networked environment, which it has called the SHARE (Systemwide Homeland Analysis and Response Exchange) Network. This is much more than a technical architecture that can be built and deployed. This is a combination of people, processes, policies, and culture, and takes full advantage of advances in information technology and the best thinking in the private sector about use of information.

Information sharing is only a starting point, not an end in itself. The Markle Task Force encouraged new ways of sharing information so that our government can get the right information to the right people in a timely way and improve our ability to prevent or respond to terrorist attacks.

Taken together, the Task Force recommendations are meant to increase the government's ability to make sense of information – to detect the indicators of terrorist activity or discover plans amid overwhelming amounts of information. The Task Force's vision is to create a trusted and distributed information-sharing environment that can enable a “virtual reorganization” of government.

The President and Congress have now adopted the recommendations suggested by the Markle Task Force, as did the 9/11 Commission and the WMD Commission. Executive Orders issued in August 2004, as well as the Intelligence Reform and Terrorism Prevention Act of 2004, adopted in December of last year, call for the creation of a trusted information-sharing environment.

Now, nearly four years after the attacks of 9/11, the stage is finally set for real and significant reform of our intelligence environment. We are on the verge of shifting from *planning for change* to *real change*.

In this new stage, implementation presents several challenges. It is essential to implement the letter and spirit of the Executive Orders and the Act in a manner that truly enhances national security while simultaneously preserving privacy and protecting sources and methods.

THREE CORE PRINCIPLES

Given the crucial period we find ourselves regarding implementation, I will devote the remainder of my talk to three key principles that should guide the implementation of an effective intelligence-sharing environment.

(A more complete set of principles and recommendations can be found in our reports and publications, which are available on the CD-ROM that was distributed here today and on our web site.)

The information-sharing environment must be developed as:

- A Distributed and Coordinated System
- A Trusted System, and
- Designed Around a Need to Share

First Principle: A Distributed and Coordinated System

The most basic principle for a successful networked environment is that information must flow in a distributed, yet coordinated way.

Currently, within the US alone, there exist some 14 federal intelligence and security agencies. In addition, there exist 17,784 state and local law enforcement agencies, 30,020 fire departments, 5,801 hospitals, and millions of other first responders on the frontlines of homeland security. Each of these has access to dispersed bits of data -- pieces of a puzzle that, if put together, could save lives. Throw in the hundreds of thousands of private entities that have similar access to data or information, and the sheer volume and spread of critical information becomes evident.

Clearly, such a distributed pattern of information holding requires a similarly dispersed system for information sharing. This is especially true when dealing with a distributed threat. Indeed, terrorists do not have a singular leadership; their decision makers and actors are similarly widely distributed.

Given that we are in an environment of widely distributed information and widely distributed threats, we will only become effective in gathering and understanding information about terrorists when the environment empowers the participation of all members of the community. Yes, every member of the community should be able to contribute his or her particular piece of information or insight for further examination, in order to understand how it may connect with the information contributed by others and users need to receive appropriate permission to use the system to search for related data. I will come back to how this can be done while preserving privacy and security of data--because immediately the specter of sharing information with terrorists comes to mind. But let's come back to this.

Information must flow through the environment in a decentralized, non-hierarchical manner. This means that users at all levels must be able to connect with other users and not be required to send information only through agency "stovepipes" or to a central hub that is responsible for redistribution. The Task Force recommendation of a "network," rather than a "mainframe" model of information flow is a critical building block of an effective information environment.

It is crucial that we begin by *leveraging existing networks*. By ensuring a certain level of *basic interoperability* between existing networks, we can begin the process of information sharing across a distributed network almost immediately.

The interoperability we seek for the longer term will require some standards to be adopted in a manner that preserves flexibility and innovation. Reference is sometimes made to lessons learned from the railroad industry. In the 1850s, railroads offered a significant advance in transportation, and several companies in North America competed for business by laying rails across the continent. Unfortunately, the railroad companies were building rails to different standards. The distance between the rails, called the gauge, varied. Some rails were 4 feet 8 _ inches apart. Some were 5 feet. Some were 5

feet 3 inches. Most trains could not switch from one network to another. The continent had multiple incompatible networks instead of one interoperable network. In the late nineteenth century, thanks to leadership from the industry and government, the American railroad industry finally settled on a gauge of 4 feet 8 ½ inches. Unfortunately, the established industry had no incentive to maintain or invest in innovation as they did in Europe and Japan – so the standards adopted locked out innovation that led to high-speed rail in these countries rather than keeping the U.S. on the leading edge.

We can also jump start the process of information sharing by using available tools such as directories, electronic pointers and indices, keyword searching, and publish and subscribe software. We need to make these tools available across the system, to all relevant and appropriate actors. These tools enable knowledge discovery and allow information to flow in many directions, and between various “levels” of the network. Needless to say, these tools must also include rules for when, and how, an actor can access information. Such rules are absolutely necessary to preserve the integrity of data. For example, rules could incorporate a requirement for an auditable documentation of a query, as well as an appeal process in case a query is rejected.

In further defining a distributed network, it is critical for a system to clearly define users’ roles and limitations. “Distributed” should not be mistaken for uncontrolled. There must be coordination that allows users to make sense of, and create a context for, the information they receive. A common concern about a distributed, decentralized system is that it would invite uncontrolled use of the system and suffer from a lack of accountability. Such use can cause the “signal” of critical information to be lost in the “noise” of irrelevant information. The Task Force does not contemplate this kind of unregulated community. It understands that all users do not have the same needs or the same ability to understand information. The system will clearly define users’ roles and limitations.

Likewise, *automatic tools* and other applications that circulate information in a more coordinated and targeted fashion can similarly increase knowledge and support analysis on the network. For example, a “publish and subscribe model,” which pushes information to various people, can be instrumental in making sure that the right pair of eyes sees the relevant information.

Second Principle: It must be a Trusted System

A distributed system is critical to effective intelligence sharing. But if that system is not trusted, both by the public and the relevant agencies, then its effectiveness will remain limited no matter how widely dispersed the network is. Government agencies and other entities must trust that information will be handled properly, in a manner that does not jeopardize national or corporate security. Critically important, the public must trust the system. The public -- including all of us -- must be confident that personal information will not be misused, and that established civil liberties will not be abused. Without such trust, any information-sharing network is likely to encounter significant opposition, both at its inception and throughout its existence. That is why our Task Force has strongly argued for the implementation of mechanisms to enhance trust from the very start of the network. Trust should be thought about now during its design or RFP phase, and not at some later point as an afterthought. I would note that this is as critical for a health information-sharing environment as it is for a national security environment.

Fortunately, several mechanisms exist to promote trust and accountability on the network.

To begin with, the network must be *built on clear, system-wide guidelines* for the collection, handling, distribution, retention, and accuracy of information. To the extent possible, these guidelines should be released to the public, and they must ensure that personally identifiable information--particularly about those who are not suspected

terrorists--is used carefully. These guidelines should provide clarity about what is permitted and what is not permitted, thus empowering officials to share information without fear of mistakenly violating rules that are less than clear. . Clear, public guidelines will also ensure that only officials with authorization can access particular pieces of information. These guidelines should be shaped by policy judgments made by politically accountable officials. Such guidelines are not primarily a statement of legal requirements.

One type of guideline that needs special attention is a requirement for *predicate-based searching*. Predicate-based searching would require officials to demonstrate a clear terrorism link in order to access personally identifiable information about U.S. persons on the network. Predicate requirements can be more or less rigorous depending on the type of information sought, and the user seeking it. In some cases, a reference to a particular investigation or program will provide the necessary predicate; in other cases--a more detailed explanation of need, or even approval, may be necessary. Overall, whenever personally identifiable information about U.S. persons is involved, searches should be designed throughout the system to favor predicate-based searching over more general pattern-based or probabilistic queries. These latter types of queries contain greater potential for misuse of personal data not relevant to a terrorism investigation—and thus hold greater potential for eroding trust in the system.

It is important, whenever possible, that content should stay with its originator, who must act as a steward for that data. This does not mean the steward can refuse to share information. It still must be accessible to authorized users in the system. What it does mean is that the entire content of a database should not simply be dumped into another entity's hands. When that happens, it becomes difficult to update the data and maintain its accuracy, and responsibility for assuring appropriate use of that information becomes unclear. This un-tethered information can become unreliable and the risk of privacy violations increases significantly. Equally important, un-tethered data can become inaccurate in ways that could in fact harm national security.

In addition to these policy requirements, one of the components of our multi-pronged strategy involves a focus on making the right technological choices. Technology, it is often said, is neutral. But this is not true. Different technologies yield different results. The design of a system is critical in determining what that system does or does not do. Therefore it is essential that the creators of any technical solution to intelligence sharing give significant thought to these considerations *before the network is created*, not after its implementation. This kind of forethought and planning is the best way of achieving policy goals like protecting privacy and other established liberties.

As indicated earlier, our network design is a *distributed network*, empowered at the edges by individual users through technologies like search directories and pointers. Our envisioned network is not a centralized repository of citizens' private transactional information. There will no big-brother database. Instead, our approach involves a dispersed network, with various pieces of information residing and collected in different locations. Most importantly, our network tightly controls that information. Law enforcement authorities in, say, a small Midwest town will not have unfettered access to the driving records of a New York resident, who may be the subject of an anti-terrorism investigation. Rather the local Midwestern legal authorities in question would instead be able to view only "pointers" indicating what types of information are available on that resident. Only if that information is deemed relevant to a counter terrorism purpose will these local authorities have access to the information itself, and only when they possess the appropriate credentials.

Conditional *access* is another key feature of our proposed trusted, information-sharing environment. Conditional access can be achieved through a range of technical solutions. As envisioned by the Task Force, an intelligence network would include a comprehensive suite of permissioning and authentication technologies, backed by strong auditing capabilities. These technologies—which would include digital rights management software, password protection, and potentially biometric

approaches—ensure that data is not simply available for the taking. It can be accessed only for a particular purpose, for a finite time, and with proper authorization.

In this approach, such important protections are strengthened by *robust auditing technologies* that track information usage both in real-time and retrospectively. These technologies, which leave a tamper-proof data trail, ensure that any misuse of the network can be identified and adequately dealt with. They provide powerful tools for ensuring accountability in access to, and use of, data. Several other technologies can play a valuable role too, including anonymizing tools, one-way hashing, and data scrubbing.

Ultimately, ongoing human oversight must supplement these technical tools but selecting the right tools is essential to achieving a trusted system, the second principle of our approach.

Third Principle: Designed Around a “Need to Share”

The government’s old paradigm of intelligence sharing was born during the Cold War, and was based on a “need to know” principle. The “need to know” principle assumes that information secrecy is of paramount concern, and restricts access to information to a select group of individuals and agencies. This principle might have been effective when the enemy was clear and well defined. But in our current situation, where threats are distributed, and where clues to attacks may lie in the most seemingly innocuous pieces of information, it is critical that a wider section of the law-enforcement and intelligence communities have access to intelligence.

This new paradigm of intelligence, designed around a “need to share” principle, does not require us to compromise on national security. One of the key challenges confronting implementation will be the need to *balance the need to share with the need to preserve information secrecy*. But it is essential to understand, at the outset, that each of these goals is critical to national security, and they are by no means mutually exclusive.

In order to achieve the necessary balance, our Task Force has recommended the adoption of a *risk-management strategy* that would help protect sources, methods, and other highly sensitive information. It is necessary to accept, however, that one hundred percent security is unattainable; a risk assurance approach that requires this level of security would place an unacceptable burden on the network. Instead, the Task Force has proposed a *layered approach* to security, which promotes sharing while minimizing risk through appropriate use of technology, policy, and oversight.

An essential tool in this risk-management strategy is the *use of tears lines*. Such tear lines can be used to separate information from its underlying sources and methods. This approach makes intelligence easier to disseminate. For example, a report could include a paragraph explaining sourcing, and then a line drawn under that paragraph, separating information on sourcing from the information itself; the contents of the report below the tear line could be shared with lower classification levels.

Technology, too, plays a critical role in promoting tear lines. As I just noted in discussing tear lines, technology can be used to electronically separate the classified portions of a report (“above the tear line”) from those that are unclassified (“below the tear line”). In addition, technology can be used to “scrub data.” Scrubbing data involves removing classified information -- such as a source’s name -- from a report before it is distributed. The various electronic authentication and authorization technologies mentioned above will, of course, also be critical in implementing the risk-management strategy proposed by our Task Force. And other innovative “e-Bay” and “Amazon” like technologies can contribute towards rating the reliability of sources as an alternative to naming them, and can suggest other interested parties and related threats based on the topics queried or the information shared.

In addition to using the right technology to “re-engineer” government, certain *cultural and organizational changes*, too, must be implemented to enhance sharing.

Indeed, the very notion of a “need to share network,” which requires a shift from our existing paradigm, requires a cultural change in the way intelligence agencies operate. Such changes can be facilitated by the use of personnel incentives, training, and other measures to counteract the cultural and bureaucratic enticements to hoard information. In addition, cultural and policy changes are required to eliminate originator controls, and more generally the sense of originator ownership, over information. On a need-to-share network, information belongs to everyone involved in the fight against terrorism. We need to minimize information silos and the compartmentalization of information.

Systematic changes to encourage collaboration will also play a crucial role. The changes could include encouragement of the creation of ad hoc analytical teams across agencies to share information and coordinate efforts. More formal arrangements can also be useful. The Task Force has recommended that certain personnel could be assigned a strategic coordinating role throughout the environment, in agencies as well as the National Counter Terrorism Center.

CONCLUSION

Achieving the principles I have mentioned represent serious challenges. We do not underestimate the difficulty of crafting the policies to guide the system, as well as the strategies needed to deploy the technology. Yet it is essential that we overcome these challenges. If we do not create plans for an information-sharing environment that achieves these principles, we will not achieve the goals set for us by the President and Congress.

A great deal of work remains to implement effectively the many actions called for to improve information sharing. We must establish clear objectives and expectations for the many participants in information-sharing efforts. We must standardize and enhance federal policies and capabilities for the analysis and dissemination of information.

Achieving the intelligence-sharing network envisioned by our Markle Task Force, and now President Bush and the Congress, will take years of dedicated and focused work.

The stakes are high, and I believe we are on the path towards real transformation of government through information sharing. The decisions we take now regarding the technical, legal, and cultural architecture of the network will have ramifications for generations to come.

The Markle Foundation is committed to working with partners in every sector and to providing assistance to the government in implementing information-sharing environments in both national security and in health care in the most effective manner. We look forward to collaborating with you as you seek to contribute to these critical national objectives.

Thank you.