Addressing Critical Public Needs in the Information Age

May 2004

MARKLE FOUNDATION

Emerging information and communication technologies possess enormous potential to improve people's lives. The Markle Foundation works to realize this potential by accelerating the use of these technologies to address critical public needs, particularly in the areas of health and national security.

A letter from the President

Zoë Baird
May 2004

Advances in information technology over the past decade have stirred the creative spirit of a generation and dramatically changed our everyday lives. As we enter the 21st century, the Internet and information technology (IT) continue to capture our imagination, holding out a future filled with possibilities that go far beyond the transformations we have already witnessed in business, education and consumer choice. Technology, woven into the fabric of the institutions that serve the public, can transform information into an ever more powerful tool that can help solve complex problems, meet critical public needs and empower people in ways that make life better for all of us.

In our recent work, the Markle Foundation has been predominantly focused on two areas where we believe IT holds great promise to create the future we have in mind: the modernization of our complex and over-burdened health care system and the strengthening of our nation's security against the threat of terrorism. These are two of the most critical issues of our time, where the benefit to be gained from the ability to put the right information into the right hands at the right time is enormous. In each of these areas, we know that the effective use of IT can literally save lives. These are areas where IT promises great breakthroughs, and where without better use of IT, our nation's goals cannot be met. At the same time, health and national security also highlight the major challenge in seeking better ways of using information: the risk such use poses to our established social values of privacy and civil liberties. We have had major collaborative efforts addressing these areas for the last two years and we plan to continue our work on the challenges presented by these two program areas for the foreseeable future. In addition, we will continue to look for similar important areas where we believe that we can have significant impact.

Markle's commitment to deepen our work in these two fields has grown out of our broader initiatives since 1999 as the Internet moved from its early uses to the mainstream. From the beginning of 1999 to the present time, the number of Internet users around the world has grown from approximately 150 million to an estimated 650 million. In this initial growth period, the Markle Foundation aimed to stimulate the participation of many needed actors to pursue the public interest potential in a variety of areas of the Internet and emerging information technologies. As we did so, we invested in these goals at a higher rate of distribution than is typical for foundations.

As the IT environment changed and the economic climate, including our own endowment, softened, we aligned our spending levels with our work in health and national security. (See Financial Section on page 14 for program spending information.) Development of the IT systems and policy direction to meet our objectives in these fields will take time and we plan to deepen our work and sustain our activity.

Improvements in the areas we are working on have the potential to be transformative. In the health care arena, imagine that you are far from home when you are seriously injured and rushed to the emergency room. Under the current system, health information remains primarily paper-based. Significant delays could occur before doctors could obtain a complete medical history from your personal physician. In the meantime, because of a lack of information about pre-existing medical conditions or medications you are taking, decisions might be made that could turn out to have dangerous consequences. On the other hand, if we transform health care to take full advantage of IT, you would be able to authorize the emergency team access to your relevant medical history stored electronically in a record that can be accessed by you from any location. The results would be dramatic—reducing the possibility of medical errors, allowing you to receive better and more efficient care and empowering you to impact the quality of your own health care.

On the national security front, the benefits of better information systems are equally striking. Consider a scenario in which federal intelligence agents and local law enforcement become aware of separate aspects of a terrorist plot for attacks on shopping malls across America. The federal government gets a sensitive intercept of terrorists discussing "malls," while local police observe suspicious surveillance of their local mall. At the same time, a manager of a department store chain with stores in many malls notices a lot of unusual social email traffic between new employees at different stores. None of these pieces of information on their own reveals a plot. Today, federal intelligence agencies protect their classified information and would release, at most, highly sanitized general warning information. Local law enforcement, lacking knowledge of the threat context, would not understand the significance of its information and would fail to share it. These potentially critical clues might be linked only in an after-the-fact investigation.

But instead, a trusted, secure network would create a regular information flow between these and the many other critical homeland security players. Rather than relying on a few analysts in Washington, ad-hoc communities would be created around common concerns. Our government needs the network and the guidelines and controls for the use of data so it can establish an information flow without legitimate public fear that our efforts to prevent terrorism will result in unacceptable intrusions on privacy.

The critical thing to underscore is that in both health and national security, these are not futuristic scenarios that require ten more years of R&D to become reality. The technology exists now or is in the development pipeline. What is needed is the collective vision and will to build the infrastructure and implement the policy changes that will make them a reality.

In both these fields, the Markle Foundation has brought together the leadership to develop and implement urgently needed solutions. We understand that these issues are complex, and that they will not be resolved overnight. But with an extraordinary group of people, we have taken the initial steps in our recent work, and are making the long-term commitment to making our nation safer and our health care better through the improved use and sharing of information in ways that protect our citizens' privacy and liberty.

To realize these visions, it is essential that progress be made on a number of fronts. New approaches to information sharing must be designed and widely adopted to enable information to flow among diverse stakeholders. At the same time, novel legal and policy frameworks must be put into place to inform and protect stakeholders and guide them in the appropriate sharing of information. Finally, while progress is being made on such key issues as identity management and the protection of data and systems, there is much work to be done using existing technologies to experiment with these new systems before truly interoperable electronic systems are ready and available to share information privately and securely, such as classified government intelligence or personal health records.

For all the potential IT holds to improve our health care and national security, it is remarkable the degree to which policy, institutional and human barriers exist and prevent creating an infrastructure that can make the most of information technology. Based on Markle's past involvement in technology policy work and our experience in mobilizing multi-sectoral groups, we have sought to address our work specifically on overcoming these barriers in order to effect large-scale institutional change.

To that end, we have thought very specifically about how the technology and policy arenas can converge to deliver information as a powerful tool to support novel solutions to complex problems – in health, national security and beyond. To put it slightly differently, while our society now has the capability to amass enormous amounts of information from a wide variety of public and private sources, information by itself is not knowledge. Our recent work in the fields of health and national security has focused on ways that discrete data can become new knowledge, directed toward public interest ends.

Health

In many ways, the United States has one of the most technologically advanced health care systems in the world. Our health care system boasts state of the art diagnostic and treatment technologies, outstanding institutions and the world's most skilled professionals. However, the picture is not so bright when looked at from the standpoint of technologies for managing medical information. Health care costs are soaring, and too many people die from preventable medical errors, more than from car accidents, breast cancer or AIDS. According to recent RAND studies Americans get the care they are supposed to only one half of the time.

The reality is that our current system is highly fragmented and, in the words of the Institute of Medicine, lacks even "rudimentary" clinical information capabilities. Vital data sits in paper-based medical records that can neither be accessed easily nor combined into a clear and complete picture of patient care. Recent advances in telecommunications and electronics have transformed much of American business and society. Yet the fundamental way in which the vast majority of hospitals and physicians gather, store and use clinical information has changed hardly at all from the days of the horse and buggy. Today, American banks (just to name one example) can move millions of dollars around the world in fractions of a second. Loan applicants who used to wait for weeks now wait mere hours for approval on the mortgage that will secure their dream home. Yet in the vast majority of hospitals, lengthy delays can occur while doctors attempt to gain access to a patient's paper records.

All of us, as health consumers, patients, parents and caregivers, feel the effects of these shortcomings in our everyday lives. Doctors must sometimes provide care without knowing the details of previous treatment or current conditions, which can lead to treatment that is redundant, ineffective or even dangerous. As patients, we lack easy access to the medical information we need in order to collaborate with our doctors in our own care. We actively want new and better ways to engage with our health care, including the use of computers and electronic personal medical records to manage our care.

According to a national poll conducted by the Foundation for Accountability (FACCT) on behalf of the Markle Foundation's Connecting for Health initiative:

- Seventy percent of consumers would want to use some aspect of an electronic medical record.
- Forty percent erroneously believe their doctors *already* use such records.
- Seventy-five percent said they would want to be able to e-mail their doctors.
- A majority said that privacy and security of their personal medical records was very important to them.

Until clinical information can be easily shared and integrated, securely and privately, our nation's health care system will continue to struggle with gaps in care, quality, safety and cost-effectiveness.

The Markle Foundation's health program is dedicated to helping break open the technological logjam in health care. Our goal is to see that the extraordinary potential of 21st-century information technology to improve the health and health care of each citizen is realized as quickly and effectively as possible.

Our most significant work in this area has been Connecting for Health: a Public-Private Collaborative. Over the past year and a half, Markle has convened a remarkable group of government, industry and health care leaders that has led the national debate on electronic clinical data standards. Early in its inception, the group drove consensus on the adoption of an initial set of standards, developed case studies on privacy and security and helped define the electronic personal health record (PHR).

"Promising developments are in the works. Connecting for Health, the health group collaborative, has come up with an initial set of data standards, developed models for protecting patient privacy and created a proposed electronic 'personal health record' to be controlled by patients, much as consumers use budgeting software to managed their finances."

Wall Street Journal, January 23, 2004

Most recently, Markle announced the second phase of Connecting for Health: the creation of a Roadmap for achieving electronic connectivity in health care. For this phase, the Markle Foundation is pleased that the Robert Wood Johnson Foundation will also be supporting our effort. The collaborative will also be developing solutions for overcoming specific barriers to electronic connectivity and then setting up a demonstration project to test solutions under real-world conditions.

National Security

The September 11th attacks exposed significant shortcomings in the intelligence structures and methods we use to protect our nation. While we knew of the threats terrorists posed, we did not fully comprehend their ability to carry out such attacks on American soil. In fact, we possessed a good deal of information that might have prevented the terrorists' plan prior to September 11th. What we lacked was a system for processing, analyzing and sharing the information in a way that might have revealed their plot. In the aftermath of the attacks on the World Trade Center and Pentagon, Markle saw a critical need to rethink the role of information and information technology in protecting our nation.

While the post-September 11 period saw many anti-terrorism initiatives unveiled, too little attention was paid to the ways in which IT could be used to improve intelligence gathering and to support better sharing of such intelligence among federal, state and local agencies and the private sector. We found there was an urgent need for policymakers, members of the private sector, academics and members of the civil liberties community to explore information needs and the ways in which existing and emerging technologies could be used to enhance our national security.

The cornerstone of our program in national security is The Markle Task Force on National Security in the Information Age. Formed in April 2002, the Task Force focuses on the question of how best to mobilize information and information technology to improve domestic security while protecting established civil liberties. The Task Force is designed to inform the policy judgments and the investments of the federal, state and local governments in the collection and use of information as it relates to national security.

To carry out that mission, we have assembled a diverse and bipartisan group of experienced policymakers, senior executives from the information technology industry, public interest advocates, and experts in privacy, intelligence, and national security. Task Force members have devoted tremendous energy and hundreds of hours of pro-bono time toward developing a strategy to increase our nation's security through the use of information and information technology.

"This impressive group of people was definitely asking all the right questions, and have come up with some very reasonable first answers…They've gotten people who normally don't talk to one another -- privacy advocates and former intelligence and national security officials -- to agree on some basic prescriptions for safeguarding civil liberties and protecting America."

Senior White House official, quoted in the *New York Times*, October 7, 2002

To date, the Task Force has poured its collective expertise and insights into two reports, both well received by policymakers in Washington and nationwide. The first report analyzed the benefits of improved information sharing between intelligence and law-enforcement communities and provided guidelines for safeguarding civil liberties in the process. The second goes further with specific recommendations for a Systemwide Homeland Analysis and Response Exchange

(SHARE) Network, which would empower federal and local officials alike to be full and active partners in protecting our security, and which would be governed by guidelines designed to protect our liberties. The initial report was helpful to policymakers as the Department of Homeland Security was being created. The second comes at a time when intelligence reform is once again at the forefront of national awareness, and when failure to make needed reforms leaves our society at risk.

> "The creation of a new homeland intelligence agency will give us a fresh chance to strengthen our freedom as well as our security. A recent study by a bipartisan commission at the Markle Foundation points the way. "
> -- Sen. John Edwards
>
> *Washington Post* Op-Ed, December 18, 2002

As the Task Force has pursued its work over the past two years, we have made remarkable progress. Our goal is nothing less than the design and implementation of an integrated, multi-agency network infrastructure for the analysis and sharing of information regarding threats to our security – as well as the policy and institutional changes that would facilitate its widespread adoption and use. We believe we have taken important initial steps that will help make America safer while protecting our cherished civil liberties. However, much work remains to be done, and the Markle Foundation is committed to pursuing these issues in our continuing effort to use information and IT to make America and the world more secure.

****

Over the past few years, the Markle Foundation has pursued a number of projects with the goal of addressing critical public needs through the innovative use of information and IT. In the process, we accomplished many specific objectives and developed a number of key partnerships in the public and private sectors. We have developed an approach that works for the many extraordinary people with whom we collaborate: convening multi-sectoral groups of leaders and innovators from technology, government, public interest organizations and business to bring about the technical and policy changes needed to enable breakthroughs in the public interest. Our partners have contributed countless hours of their time to our common goals. We are grateful to them for choosing to work on these issues with us.

Over time, this approach to Foundation operations allows us to contribute to large-scale, sustainable change that far exceeds the dollars we apply to the problems we have chosen to address. This model also enables us to tackle issues that are ripe for change at the point in time when we believe we can have the most impact. We have found that the most effective way for us to leverage our resources is to structure and operate our own projects in cooperation with our partners instead of working as a traditional grantmaking organization.

We have used this approach in recent years to tackle a number of important issues. For instance, we designed and implemented a variety of interventions to achieve public interest outcomes in IT policy. We facilitated and promoted transparent, accountable, multi-sectoral policymaking processes through which government, industry, and non-profits could work together to develop legitimate IT policies that serve the public interest in a variety of non-traditional venues like the Internet Corporation of Assigned Numbers and Names (ICANN) and the Group of Eight (G-8) summit in 2000. We developed the first major use of the Internet in presidential elections in 2000 in a collaboration between the major portals, news organizations and non-profits. And above all, we built and fostered IT policy capacity among a number of public interest representatives and non-governmental organizations (NGOs) -- domestically and globally -- so that they can continue to bring public interest concerns to decisions about major issues in a variety of venues and further develop effective solutions. (See Program Highlights on our website at http://www.markle.org for additional details).

Because we have been operating these and other programs, we have funded few unsolicited proposals for some time. We have decided formally to discontinue accepting unsolicited grant applications. For the time being, we expect to focus on our health and national security programs.

In my first letter as Markle's President in 1999, I noted the transformative potential of the Internet and other developing information technologies. It is hard to believe now that at that time most people were just becoming familiar with the Internet. *The Wall Street Journal* wrote in November 2002 that in the summer of 1999, "we wanted to introduce readers to this strange animal called the Web."

Now, five years later, I think we all have a much better idea what the Internet and related advances in technology can contribute to our societal achievements. We now understand how technology can help transform information into knowledge and how that knowledge can be used in new ways to address some of our most pressing social problems.

I concluded my 1999 President's letter by expressing the hope that in the years ahead Markle would be able to improve life in the Information Age. Looking back, I believe we have made a difference, and I also believe that there is much more that Markle can contribute. Through continued innovation and dedication, Markle and our many partners will continue our work toward goals that none of us can achieve alone. Together, we can contribute to solutions for critical public needs by leading in the use of information technologies.

Sincerely,

Zoë Baird

Health

The overarching goal of the Markle Foundation's Health program is to accelerate the rate at which information technology enables consumers and the health system that supports them to improve health and health care.

The effective use of IT in health care presents an opportunity to move critical medical information where and when it is needed in a secure and private manner. The Markle Foundation's health program is dedicated to ensuring that the primary beneficiary of this opportunity is the patient. Bringing electronic connectivity to health care has the potential to empower patients by allowing them to control their own medical records in a secure and private manner. Medical records could be accessible according to the needs of the patient, accessible even if the patient changes doctors, hospitals or health insurers. Such a system would allow patients to become more active participants in their own health care, creating a new and powerful partnership between patients and physicians. In addition, such a system would also improve the quality of care, reduce medical errors and help stabilize the rapidly raising costs of health care.

However, a number of challenges must be overcome to enable the health care industry and patients to take advantage of the full power of modern technology. These barriers include the lack of interoperability between systems, privacy concerns, the fragmented nature of the industry, misaligned incentives and a legal framework that may not facilitate the use of IT. The Markle health program works to eliminate these barriers so that we can realize information technology's potential to improve health and health care for every individual.

Over the last few years, Connecting for Health has played a key role in Markle's health strategy. Connecting for Health, a public-private collaboration of over 100 stakeholders from across the health care sector, seeks to create an environment that brings the innovation and expertise of the private sector together with the public sector to help drive our health care system toward a common goal of interoperability.

Connecting for Health's goal is to serve as a catalyst for changes that would begin to clear the way for an interoperable health information infrastructure. It was designed to address the challenges of mobilizing health information in order to improve quality, conduct timely research, empower patients to become full participants in their care, and bolster the public health infrastructure. The success of Connecting for Health's initial phase, which broke through the long-standing impasse related to data standards, was attained by finding achievable milestones and focusing on areas where consensus could be achieved.

> *"(Connecting For Health's) initiative has enabled the Government to work with the private sector in planning how to make the most use of technology to improve health care for all Americans."*
>
> *HHS Secretary Tommy Thompson*
> June 5, 2003

Connecting for Health's Steering Group, whose members represent a driving force in health care, agreed for the first time at its initial meeting in September of 2002 on the voluntary adoption of an initial set of data standards and communication protocols for the sharing of health care information. The U.S. Government announced its adoption of these same standards in March of 2003.

Connecting For Health's achievements in just nine months toward the adoption of health care data standards represents progress that has eluded the health care industry for more than a decade. Connecting for Health:

- Built consensus on an initial set of health care data standards.
- Developed case studies of places where privacy and security practices may provide a model for others.
- Advanced our understanding of the consumer's role in an interconnected health care system by defining the personal health record and its use.

Since September of 2002, the importance of interoperability to health care safety and quality has been publicly endorsed by leaders including President Bush, Secretary of Health and Human Services Tommy G. Thompson, U.S. Food and Drug Administration Commissioner Mark B. McClellan, and by leading Members of Congress of both parties.

Connecting for Health's action-oriented agenda, meanwhile, has drawn wide support. It was recently announced that its work will continue in a second phase in which we will focus on developing an incremental Roadmap to achieving electronic connectivity. The Roadmap, which will be based on the results of several high-level working groups, will detail an action agenda of achievable objectives over the next twelve months that will leverage activities between public and private health care sectors toward an interoperable health information infrastructure. Connecting for Health also plans to conduct a demonstration project to test and evaluate the Roadmap.

Connecting for Health Conference, June 5, 2003

For more information on Markle's Health program, please visit www.markle.org. For more information on Connecting for Health, please visit www.connectingforhealth.org.

National Security

During the Cold War era, the use of intelligence information was dominated by a culture of classification and tight limitations on access, in which information was shared only on a "need to know" basis. Law enforcement, similarly, restricted access to information to protect the prosecution process. And our nation drew a line at the border, applying different rules to our government's activities offshore from those we applied at home. That structure was appropriate for a different time. However, it is imperative that we move to a different approach if we are properly to address the threat our nation faces now from terrorism.

The threat we face today requires unprecedented speed in the way the government collects, shares, and acts on information. In fact, information has become the key to enhancing our nation's security. The events of September 11th 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. To deal with this new threat, information needs to be tailored to facilitate decision-making and action at all levels—not only by the President, but also the police officers on the street.

The Task Force's first report, *Protecting America's Freedom in the Information Age*, received the International Association of Law Enforcement and Intelligence Analysts 2003 Professional Service Award for "the most significant contribution to the literature of law enforcement and intelligence."

At the same time, the new information requirements must be developed in a new framework of civil liberties protections. These are not competing interests to be traded off, but complementary goals to be developed through wise policy and new technology tools.

Exploring how information and information technology (IT) can enhance our national security is an issue with which the Markle Foundation has been engaged since 2000, when we began to examine the national security implications of a world increasingly interconnected through technology. In the wake of the attacks of September 11th, the Markle Foundation formed the Markle Task Force on National Security in the Information Age to find ways in which information could be better used to enhance America's security while protecting our liberties. We recruited as members some of the nation's foremost authorities on national security who served in the Carter, Reagan, Bush and Clinton Administrations, as well as leading experts on information technology and civil liberties.

In October 2002, the Task Force issued its first report, *Protecting America's Freedom in the Information Age*, which identified the ability to share information as the most urgent task facing government in protecting the homeland. The report proposed a plan for a distributed IT network to share terrorism-related information among federal, state and local government agencies and the private sector so that threats could be identified and prevented. In addition, the report provided a framework for considering how the government might make most

effective use of data residing in the private sector, while preserving liberties and avoiding the imposition of undue costs on businesses. It has had a significant impact on the debate about how to create a national security information system and was helpful to those involved in the creation of the Department of Homeland Security.

In December 2003, the Task Force released its second report, *Creating A Trusted Information Network for Homeland Security*. The report concluded that by using currently available technology, the government can set up a network that substantially improves our ability to prevent terrorist attacks and protect civil liberties. It provided details for the necessary elements of a proposed System-wide Homeland Analysis and Resource Exchange (SHARE) Network that would more effectively combat terrorism than our current system, while protecting privacy.

> "As he begins his tutorial on homeland security, [Chairman of the House Select Committee on Homeland Security Congressman Chris] Cox touts a recent report by the Markle Foundation on data systems as required reading…"
>
> *The National Journal*, April 5, 2003

The public's trust in a governmental network that makes use of information about its own people can be achieved only if government-wide guidelines for information sharing and privacy protection are established after open public debates on the issue. The Task Force therefore proposed that the President set the goal of creating such a network, and issue clear government-wide policy guidelines for the collection and use of information, including private sector information.

There is no question that leveraging information technology can help us fight the war on terrorism more successfully. However, to achieve this, our nations' policy makers must first set the goal of using technology to preserve and enforce our values as well as to collect and share information.

Task Force Meeting, July 2003

Going forward, the Task Force will continue to work on these challenges. It will focus on helping the U.S. government and industry assess their readiness for and provide tools to implement the next generation information sharing initiatives. Furthermore, it will also pursue further work on privacy guidelines and the handling of private sector data, to create better understanding of the potential new borders on collection and use of information.

While terrorist threats remain high, it is critical that information collection, sharing and analysis initiatives are implemented on a solid foundation of strategy and planning. The Markle Task Force will work towards providing effective ways to build such a foundation.

For more information on Markle's National Security program, please visit www.markle.org. Additional information on the Markle Task Force on National Security in the Information Age can be found at www.markletaskforce.org.

Syncing Technology with Sociology

Socio-intranet: productivity's next frontier

By Michael O. Leavitt, Former Utah Governor, Administrator of the United States Environmental Protection Agency

Occasionally, I am asked what part of my job as governor I enjoyed most. It's an easy question to answer: I treasured the opportunity to stand, for a time, in a place of sufficient perspective to see disparate streams merging together to form the river we call society.

From this vantage point, I sense an important development in the way technology and sociology are shaping our world. *Two predictions*: First, interoperability will become as familiar in the next decade, as network was in the last. Second, a new kind of sociology will partner with technology to become the catalyst for improving productivity.

What is interoperability? It's the ability of one system to benefit from another. I carry a PDA built by one vender that syncs with applications on my desktop, built by another. That process of "syncing" represents the most basic form of interoperability.

The second level of interoperability is often called "systems integration" or "enterprise computing." This kind of interoperability uses the Internet to sync entire technology systems so they can exchange data and communicate in ways that dramatically increase productivity. This is what happens when the health department "syncs" technologically with public safety agencies to improve services for the community.

The highest level of interoperability and the next frontier in national productivity is what I call a "socio-intranet." Socio-intranets require large-scale technological integration as well as masterful collaboration among private and public organizations that normally compete in the marketplace or have other conflicting interests. It is similar to what Ray Noorda, founder of Novell, a pioneer in networking, called "coopetition."

Our nation's effort to create a national homeland security plan is a good example of where a socio-intranet will be necessary to accomplish our task. Making the national government, state and local law enforcement, health and transportation, and the banking industry interoperable is a staggering task both technologically and socially.

Over the last five years I have been involved in several interoperability projects that were large enough in scale to be considered socio-intranets. And in every case it was the sociology that formed the major impediment to progress. There were rigorous debates and discussions about the role and power of government. There were partisan politics and personal business jockeying. There were egos and turf.

So, as I look to the future and see the inevitable confluence of technology and sociology, I can see that our biggest challenge is not new technology, but new sociology. We have the ability to make the machines work together, but what about the people? Getting technology and sociology to sync is the next frontier, our next great challenge, and this generation's opportunity.

Tackling the Challenge of Digital Identity

By Esther Dyson, Chairman, EDventure Holdings, Founding Chairman of ICANN

What does digital identity mean at the beginning of the twenty-first century? Even as governments and businesses get better at generating and recording information about individuals, individuals are becoming rightly more concerned about controlling the data proliferating about themselves.

But the issue isn't as simple as giving individuals control over all information about themselves. Such control may conflict with other interests, including the rights of other individuals to speak freely, the rights of the public to know the truth, a general public interest in security, and various other interests, including governments' interest in reaching its citizens and getting them to pay their taxes.

None of these conflicts is particularly new, but the proliferation of data and the tools to find it seems to change the rules of the game. Throw into the mix the strong reaction to September 11, and we do have a new environment.

In addition to data knowingly collected by businesses and government, and more or less knowingly volunteered by individuals, we now have a world of "slime trails" visible to others. The e-mails you write, the Websites you visit and post at, what other people say about you in their blogs…all that stuff is around. Most of it gets lost in the noise but here is the difference it is much easier to reassemble. Everyone has the ability to be "famous" on Google at the whim of someone else. There's a lot of public information available about the average person.

Unfortunately, right now the public is both paranoid about many identity "threats" such as identity theft and general breaches of privacy and woefully underinformed about its own abilities to control personal information.

The solution to personal control over identity does not have a single answer. Some trade-offs need to be determined by government or some social convention. Others need to be surfaced by the market, ideally offering service terms and contracts and policies that meet a variety of individual preferences rather than assuming that one size fits all.

Markle could play an important role both in advising governments and in sponsoring models for businesses and other private organizations to follow.

On the government side, it has already done seminal work through the Task Force on National Security in the Information Age. Rather than high-sounding platitudes about the trade-offs between privacy and security, the Task Force came up with some concrete examples of how the trade-offs in principle can be applied and conflicting interests reconciled in practice.

In the private sector, consumers and individuals have more power than they know. They have the ability to withhold their data or to take their business elsewhere. But businesses need to see a demand for different policies concerning customer data, and they need help in formulating and communicating such policies effectively.

Most such policies are unintelligible to normal people, so it's impossible for the market to reflect the latent demand for them. Simply educating people – both consumers and those who run institutions that collect and manage data – could help a lot.

The first step towards better handling of all the changes surrounding digital identity is to make it clear what it is and what you can do with it. Then individuals can decide what they want, and make the choices for themselves.

Connecting for Health

By Herbert Pardes, M.D., President and CEO
New York–Presbyterian Hospital

When we and others spoke to the Markle Foundation about information technology interoperability and health care, they responded in force. "Connecting for Health" was created and less than a year later a working team presented findings and recommendations for standards.

This is the type of action you expect from the Markle Foundation, which has staked a leading role in information technology thought and leadership. Health care has been in need of direction on information technology for some time. Our medical tools and pharmaceuticals are highly advanced, but the systems to bring them together for monitoring, diagnosis and treatment are almost primitive. In fact, the routine transfer of data, which should be automatic, may still require pen and paper in most modern hospitals. Each time it is handled it invites "clerical errors" that compromise our nation's health care. The rewards of such a unified system would be considerable. Health care would have access to the proper information to care for a patient no matter where the patient is. But sophisticated patient records now exist in less than 10 percent of hospitals and few of those hospitals can share records between them.

Standards are the answer. And the barriers to standardization, without the right leadership, could be insurmountable. It must be practical in a hospital setting. It must be doable with current technology. Industry must agree to support it. Hospitals, with government support, must be able to afford it.

With standards in place, information between hospitals can be shared to act as an early warning system for examples of bioterrorism or epidemic. By monitoring several hospitals at once, an integrated medical system could help public health officials recognize patterns of a health emergency sooner than they might otherwise.

Why is an integrated system so important? Because better integration allows systems to communicate and prevent errors, protecting patient health. It could mean a significant difference for patients. According to estimates of the Institute of Medicine, more than 44,000 people can be expected to die from medical errors this year - greater than the number of people who die each year in automobile accidents.

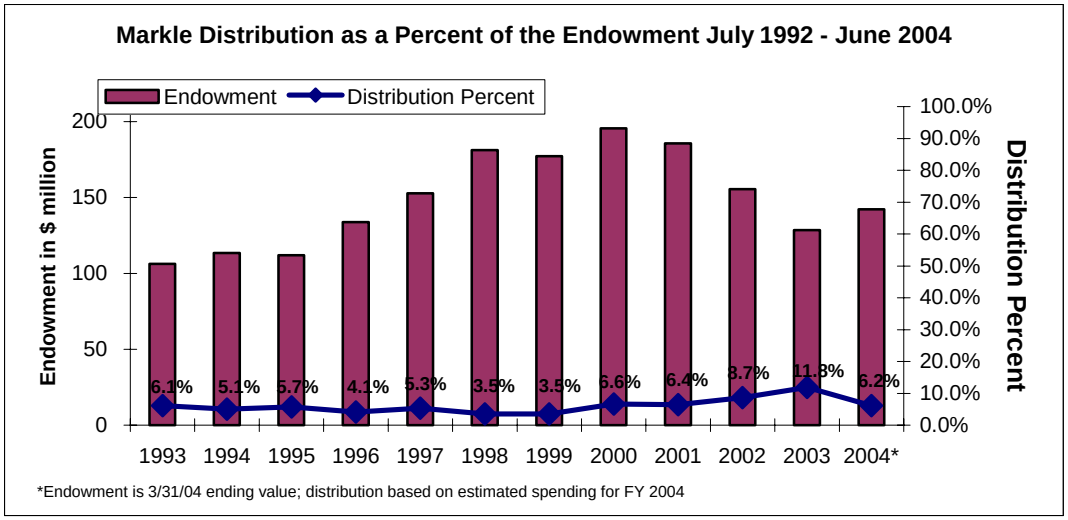
The Markle Foundation brought all the right people to the table to address problems and look for solutions. With industry, hospitals, technologists, and public policy experts together, issues that had been unsolvable became manageable and doable.

At a recent conference, the work of this group was announced and practical standards were recommended and adopted by the members of the group. These same standards will become the future of patient data within hospitals and in systems created by industry.

This is a remarkable achievement in a remarkably short period of time and one that will directly benefit patient care. It will bring consistent care throughout our hospitals. Our doctors, nurses and medical staffs will have the information and checks they need to provide patients the best possible care.

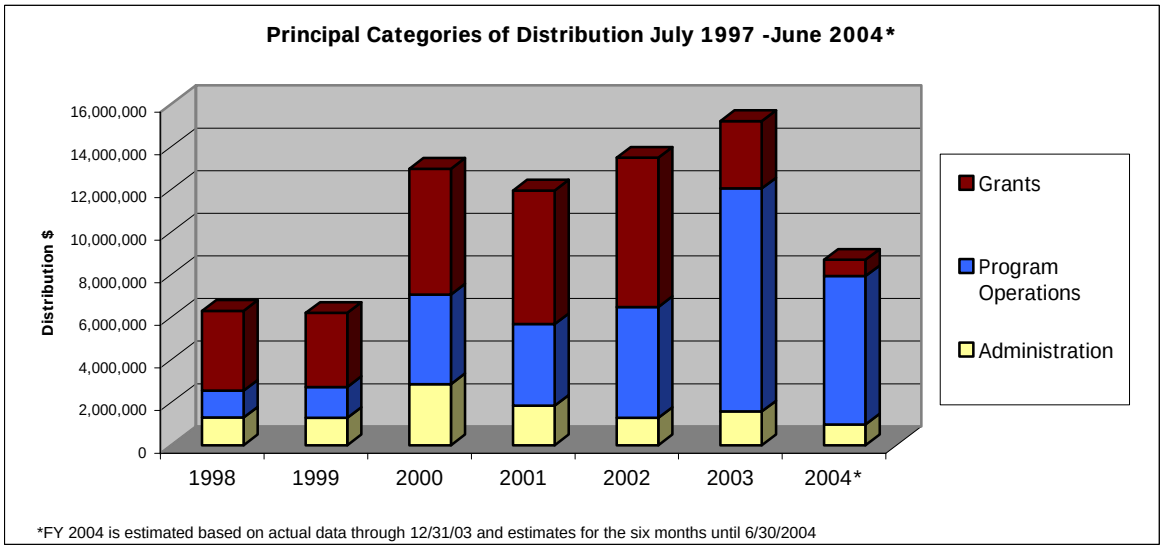
Interoperability is not a glamorous subject in the manner of curing cancer or therapeutic cloning. But because it can impact on every other aspect of health care, it has the potential to save more lives. Recognizing the importance of this potentially arcane subject is but one of the things that marks the Markle Foundation as a leader.

DISTRIBUTION AS A PERCENT OF THE ENDOWMENT



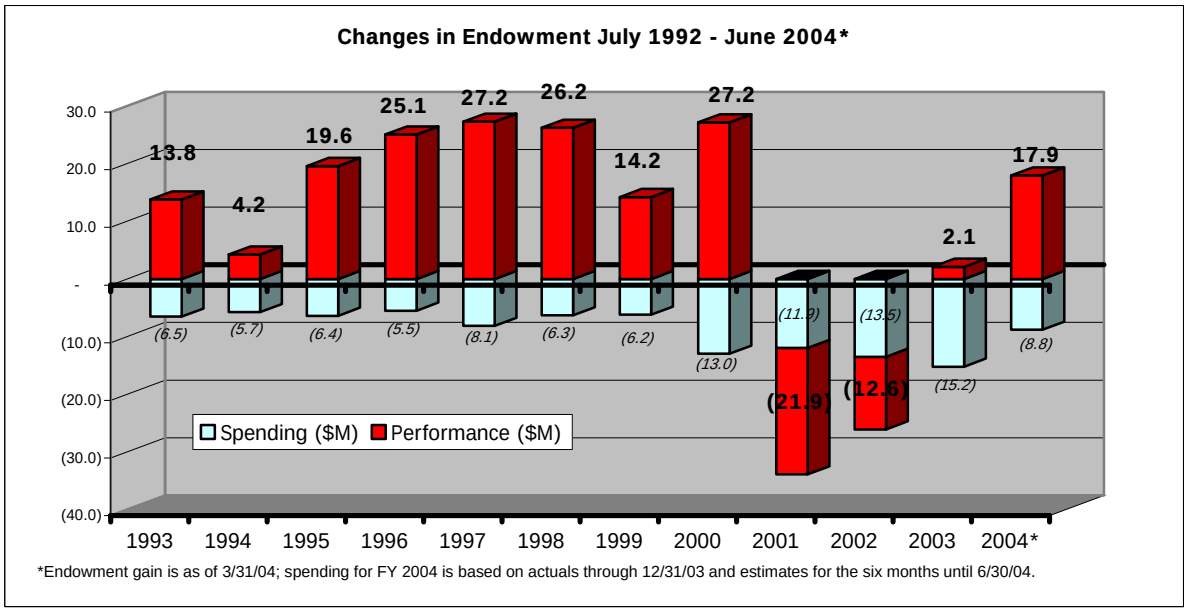
- The foundation's distribution (spending on program and administration) is shown on this chart as a percent of the foundation's endowment for the period FY 1993 to FY 2004 (July 1992 – June 2004). Appropriations decisions are made based on programmatic needs and distribution lags appropriation decisions.

PRINCIPAL CATEGORIES OF DISTRIBUTION



- The above chart, compiled from data on Markle's tax returns (990-PF), shows Markle's distribution for the period FY 1998 – 2004 divided into three categories: Grants; Program Operations; and Administration.
- Funds budgeted for distribution grew in FY 2000, reflecting the commencement of a strategic plan which called for accelerated project development at a time when information technology and Internet policy were rapidly being adopted
- Increases in Program Operations reflect the Foundation's transition away from grant-making and toward direct operation of projects.

CHANGES IN ENDOWMENT



*Endowment gain is as of 3/31/04; spending for FY 2004 is based on actuals through 12/31/03 and estimates for the six months until 6/30/04.

- Over the last twelve years, Markle's endowment has fluctuated between $100 - $200 million; this chart shows endowment performance (net income, gains and losses) in red and distribution in blue.
- From FY 1993 – 2000, the endowment nearly doubled in value, principally because of substantial investment gains.
- From FY 2001 – 2003, the endowment declined in value, principally due to declining investment results. Distribution in this period was also at the higher level established in 1999 for FY 2000 forward.
- In FY 2004 the endowment is again showing significant positive returns (the data shown are through 3/31/04), and projected distribution for the year is significantly reduced.
- In FY 2004, distribution has been targeted at the level of our national security and health work, which we expect to be our principle focus for the foreseeable future.

Financial Statements

STATEMENT OF FINANCIAL POSITION

as of the period ended June 30,	2003	2002
ASSETS		
Cash	282,122	1,842,644
Investments at Fair Value	129,227,749	141,565,543
Program Related Investments	610,438	667,438
Receivables and Other Assets	188,269	152,492
Prepaid Exise Tax	85,000	85,000
Net Fixed Assets	2,419,935	2,697,163
Security Deposit	980,000	980,000
TOTAL ASSETS	133,793,513	147,990,280
LIABILTIIES		
Project and Grant Appropriations payable	2,357,434	4,012,611
Accounts payable/Accrued expenses	111,944	365,550
TOTAL LIABILITIES	2,469,378	4,378,161
NET UNRESTRICTED ASSETS		
Contributions	17,071,767	17,071,767
Accumulated Revenues and Investment Gains	112,249,298	112,422,885
Unexpended Project Appropriations	2,003,070	14,117,467
TOTAL NET ASSETS	131,324,135	143,612,119
TOTAL LIABILITIES AND NET ASSETS	133,793,513	147,990,280

STATEMENT OF ACTIVITIES

for the year ended June 30,	2003	2002
REVENUES		
Interest and Dividends	2,433,106	3,680,829
Realized Capital Gains (Losses)	(14,075,351)	(15,507,194)
Net Partnership Income	931,211	612,637
Other Income	4,382	-
Investment Expense	(859,913)	(796,310)
Tax Expense	-	(40,000)
NET REVENUES	(11,566,565)	(12,050,038)
EXPENSES		
Grants Expense Net of Refunds and Cancellations	1,655,297	5,706,189
Program Operations	10,190,645	5,862,658
General and Administrative Expense	1,582,613	1,027,708
TOTAL EXPENSES	13,428,555	12,596,555
Unrealized Gains/(Losses) on Investments	12,707,137	(548,173)
Increase/(Decrease) in Net Assets	(12,287,983)	(25,194,766)
Net Assets, beginning of Year	143,612,119	168,806,885
Net Assets, end of year	131,324,136	143,612,119

Note: Audited Financial Statements are maintained at the Foundation.

BOARD OF DIRECTORS

Joel Fleishman
Chairman

Zoë Baird
President

Lewis W. Bernard

Tom A. Bernstein

Raymond Clevenger III

John Gage

Lewis B. Kaden

GG Michelson

Peter A. Nadosy

Herbert Pardes, M.D

MANAGEMENT

Zoë Baird
President

Karen Byers
Managing Director
Chief Financial Officer

Carol Diamond
Managing Director
Health

Todd Glass
Director of Public Affairs

Anna Nigido
Director of Finance and Administration

Stefaan Verhulst
Chief of Research

This report supplements the continuously updated material on our web site, www.markle.org, where we provide more information on our work in recent years and our commitments for the foreseeable future.