James A. Baker III Institute for Public Policy
Rice University

# Information Technology Policy: Recommendations for the Next Administration

By

Christopher Bronk, Ph.D.

Fellow in Technology, Society and Public Policy
James A. Baker III Institute for Public Policy
Rice University

December 19, 2008

These papers were written by a researcher (or researchers) who participated in a Baker Institute research project. The research and views expressed in these papers are those of the individual researcher(s), and do not necessarily represent the views of the James A. Baker III Institute for Public Policy.

## Overview

This paper advocates that the next U.S. administration place a renewed emphasis on information technology (IT). It has been more than a decade since speculation about "information superhighways" and "bridges to the twenty-first century" dominated the political terrain. We should now form pragmatic policy regarding IT development and application.

- ***Recommendation 1:*** Appoint a federal Chief Technology Officer (CTO) as a steward for private investment, public-private partnership building, and application in government. While a CTO will likely oversee many areas, IT will remain a primary focus. The United States must remain a global leader in IT if its standing in the community of nations is to be assured.
- ***Recommendation 2:*** Repair the nation's cyber-infrastructure. An economic stimulus measure directed at the nation's crumbling bridges and roads should similarly address the links and nodes of America's cyber-infrastructure.

Under the general categories of private, public–private, and government (public) initiatives, the following ten items could produce economic benefit, enhance societal and national security, and improve the way the federal government functions. These categories are meant as a starting point and are neither comprehensive nor mutually exclusive.

- ***Recommendation 3:*** Private sector initiatives
  - *3.1:* Build new pieces of telecommunications infrastructure that focus on wired and wireless broadband technologies.
  - *3.2:* Invest in energy-efficient, sustainable green IT designed to mitigate IT's carbon footprint.
  - *3.3:* Develop computing technologies, both hardware and software, to assure the survival of Moore's Law for another generation.
- ***Recommendation 4:*** Public–private initiatives
  - *4.1:* Form partnerships to implement IT in health care, focusing on the implementation of electronic health records.

  - *4.2:* Develop industry and regional communities that can help secure public and private cyber-infrastructure.
  - *4.3:* Partner industry and academia to inject rigor, resources, and opportunity into the public school system in order to train a new generation of computer engineers.
- ***Recommendation 5:*** Government IT initiatives
  - *5.1:* Create a new U.S. Department of State entity to engage in digital public diplomacy.
  - *5.2:* Overhaul the federal IT workforce by recruiting and training a cadre of technical managers capable of working with industry to design and implement programs on time and within budget.
  - *5.3:* Construct new interactive Web 2.0 information communities, modeled on Intellipedia, that are managed by government but incorporate information from outside sources as well.
  - *5.4:* Enunciate a clear national policy on monitoring the Internet and digital networks to provide actionable intelligence and construct a safer digital society.

## Background

The United States has been a dominant force in IT and telecommunications since Samuel Morse patented the electrical telegraph in the 1830s. In subsequent decades, a succession of American companies—including Western Union, AT&T, IBM, Microsoft, and Google—have led the field, producing innovative technologies that have benefited shareholders and the U.S. economy alike. Today, U.S. firms—Google, Microsoft, Oracle, Cisco, and Hewlett Packard among others—still hold the high ground in global IT. The question is, for how long?

With the U.S. in the most serious financial crisis since the Great Depression, how might the government intervene to spur technological development and economic activity? An answer may be found in the spirit of the Communications Act of 1934 which, among other things, turned the concept of universal service into law by helping to make phone service widely available.

At the dawn of the twentieth century, pundits argued whether every American household or business needed a telephone. A century later, the folly of any argument against telephone connectivity is clear. The same might be said for connection to the dominant network of our day: the Internet. In hindsight, the Communications Act can be viewed as a stimulus for the telephone industry, which saw its customer base shrink drastically as a result of the Great Depression. Government intervention on behalf of the IT industry during the current economic crisis could be similarly beneficial. A move to make the Internet universally available could spur technological advances and reinvigorate the economy.

We urge the United States to firmly re-establish itself as the global leader in IT, largely by the same set of drivers that got it there in the first place. Initiatives for innovation, development, and adoption of IT are divided into three general categories:

1. **Private** initiatives, in which government serves as venture capitalist and stimulation vehicle for activity that would not otherwise take place under market conditions.
2. **Public–private** action, where industry and government partner to work on problems that neither is capable of solving independently.
3. **Public** initiatives, or actions taken by government to adopt IT to improve or revolutionize its business processes, from human resources to intelligence collaboration.

## Recommendations

### *Recommendation 1: Federal Chief Technology Officer (CTO)*

Since the appointment of a federal Chief Technology Officer (CTO) is a likely objective of the next administration, we advocate that the Office of the CTO be subdivided into three operational areas: (1) a venture development firm; (2) a government to non-government liaison; and (3) a technology review body for government. While both the Clinton and Bush administrations opted against the creation of a federal Chief Information Officer (CIO), the current economic crisis has led to an atmosphere more open to the possibility of new governing bodies.

Guideposts for the role of a CTO in industry are few, however. The federal CTO should have the funds, mandate, and administrative capacity to develop new initiatives in IT and beyond, from nanotechnology and stem cells to open-source software and a next-generation Internet. The CTO should also have the authority to tap expertise from government and industry to solve problems, such as cybersecurity or broadband penetration, and overhaul the information-management component of government. Finally, the federal CTO should address the glaring need for an overhaul in the education of our future workforce, whose mastery of science and math—the foundation disciplines for careers in IT—is very poor.

***Recommendation 2: Government as a Venture Capitalist***

With the American taxpayer now a stakeholder in the investment-banking sector, it makes considerable sense to find ways to make similar investments in technology. Naturally, without a clear concept or business model, the federal government does not wish to replicate the hyperbolic investments made during the dot-com era. That said, we must recognize that while the United States hedged its stake in the information revolution, most international competitors redoubled theirs.

The quick launch of a federal technology venture capital operation will permit the sort of innovation needed to regain ground in the global competition for leadership in IT. Countries that surged forward in the past decade were aided by collaborations between industry and government. In India and China, there is private and public investment in university computing and telecommunications programs. Morse, Edison, Gates, or Brin may opt for Bangalore or Shanghai over Silicon Valley as the venue for his or her firm. This would have significant geopolitical consequences for the United States.

***Recommendation 3: Investments in the Private Sector***

*3.1: Universal Service – Final Mile Fiber, Wireless, and Municipal Connectivity*

While local government initiatives to provide wireless Internet service at low or no cost have largely foundered, there is a clear need to construct high-bandwidth connections for more households and businesses in the United States. The problem for even the largest telecommunications players is the timetable necessary to recoup investment. Laying fiber-optic cable is very expensive. But if America is to have a world-class information infrastructure, it will require a network that delivers fiber-optic performance not only on long-haul connections between cities, but in neighborhoods as well. *A broadband/wireless infrastructure fund* *temporarily managed by the federal government could pay for networks that would otherwise not be built, and leave them to be managed in the best hands: the private sector.*

### *3.2: Green IT*

While estimates vary, it is generally accepted that the IT sector produces about 2 percent of all carbon emissions on the planet today. A decade from now, the estimate will rise considerably as computers and devices become more powerful, consume more energy, and find more users. The goal is efficiency. Resources should flow to firms able not only to increase data processing or transmission with a fraction of the power, but also build IT that is efficient in other sectors, from manufacturing to home energy use. We should look for the wireless provider that can bring a mobile device to market that has a battery life of not a day or week, but a month or more. *A green IT initiative, including a reinvigorated government energy-saving program such as EnergyStar, should be part of any federal technology policy; it could spur industry to make the sorts of devices the marketplace wants and the environment needs.*

### *3.3: Next-Generation Computing*

Moore's Law, the idea that computer-processing power doubles every eighteen months, has permitted the movement of 1980s supercomputing performance to the contemporary desktop. Engineering elements that have propelled this constant doubling and redoubling of processing power now offer diminishing returns, and others have hit practical walls. Parallel computing—the task of harnessing multiple processors or cores—is the obvious next step. However, this requires a broad reengineering of software. *The federal government should fund academic and industry research that will preserve Moore's law and produce the software necessary to exploit parallel computing across dozens, hundreds, or millions of processor cores.*

## ***Recommendation 4: Public–Private Initiatives***

### *4.1: Health Information and Computing Technology (ICT)*

Former Secretary of Health and Human Services Tommy Thompson once remarked that "the most remarkable feature of this twenty-first century medicine is that we hold it together with nineteenth-century paperwork." Private firms, large and small, have moved to supply digital information systems to hospitals and large clinics. However, the capacity for those institutions to communicate with one another and with the smaller ambulatory practices, which still largely use paper records, remains limited. The result is an environment in which physicians make decisions in information-poor conditions and paper shuffling comes at an enormous cost. Nonprofit entities may be able to serve as a trusted third party, broker, and intermediary in the digitization and security of health data that is portable, current, and available when needed. *Government should foster interoperable standards for digital information transfer, spur nonprofit health IT operations, and subsidize the implementation of ICT systems in small practices where most Americans still receive primary care.*

### *4.2: Cybersecurity*

Despite enormous investment by government and industry, no satisfying answer exists for the question, "In information security spending, how much is enough?" Reports of data breaches and potential vulnerabilities regularly make news, yet efforts to secure the cyber-infrastructure remain incomplete. The government has provided guidance to infrastructure operators and software developers, but vulnerabilities remain at an unacceptable level. We argue here for NGOs (including academia) to partner with the government to form information-sharing coalitions to address the information security problem. If the federal government—and in particular, the Department of Homeland Security—is to get serious, then it must move beyond a top-down approach. Developing knowledge-sharing communities that cross government-industry boundaries may help resolve the issue. *A non-government information security organization staffed largely with part-time civilian reservists and headquartered in Silicon Valley, with offices across the United States, would take the country a step forward in securing its cyber-infrastructure.*

### *4.3: Technology Education*

While America's universities remain among the world's finest, drawing scholars from every corner of the globe, the public education system that prepared the majority of students at the country's top colleges is now in crisis. The bill for years of falling math and science proficiency, rising dropout rates, and failed efforts to prepare young people for the workforce has come due. Teaching civics and preparing students for an assembly-line economy simply is not enough if the U.S. is to remain competitive in technology. If U.S. universities and corporations are to continue to access homegrown talent, they must assume a greater role in fixing broken schools. IT will have an important part in such an effort. *A government program that compensates private firms and universities for providing the educational resources necessary to produce a new generation of computer and electrical engineers would improve America's ability to compete internationally and produce the sort of innovation essential for the economy.*

***Recommendation 5: Federal Government IT Initiatives***

*5.1: Digital Diplomacy*

During the Cold War with the former Soviet Union, President John F. Kennedy named journalist Edward R. Murrow to lead the United States Information Agency's (USIA) efforts in public diplomacy. The USIA's functions were transferred to the Department of State in 1999 when the agency was disestablished. While argument over the wisdom of this decision continues, the number of venues for the practice of public diplomacy has continued to grow. Although USIA-run libraries once served as a beacon, the Internet now brings mass connectivity to billions in the developed and developing worlds. Internet cafés in the Middle East may be both vehicles for societal development and cybermadrassas. The United States needs an innovative way to engage in public diplomacy in cyberspace. *We recommend the creation of a Center for Digital Diplomacy at the Department of State, where U.S. diplomatic professionals could work with America's immigrant population to send a clear message that the U.S. is present on the world stage and listening.*

*5.2: Government's IT Management Workforce*

The greatest single threat to the federal government is its inability to cope with complex design and production. Huge sums are invested in federal IT, but some government managers are seemingly unable to buy or successfully build large, complex systems. The intelligence community's reconnaissance satellite program, the FBI's case management software, and a host of other information management projects have foundered because those charged with their management lack the ability to communicate their needs and work with industry to deliver the product. While the contractor community is also culpable in these failures, blame can be shared. *The U.S. government needs to develop a cadre of IT managers skilled in both systems development and integration and program management. These managers should be trained to* *direct the actions of skilled contract personnel and be paid at near-private industry levels. Scholarships and favorable loan-repayment terms should be offered to individuals who have or are inclined to develop the necessary skills.*

### *5.3: More Web 2.0*

The greatest single achievement in intelligence community (IC) reform since the terror attacks of September 11 has been the implementation of Intellipedia. Intellipedia is a Web 2.0 wiki system patterned after the hugely successful Wikipedia. It has been used as a vehicle to break the severe stovepiping found in the IC. In addition, Intellipedia has been employed in the creation of the highest value intelligence products, including the National Intelligence Estimates. The federal government needs to expend more effort to improve information sharing across agencies and different levels of government and non-government actors. *We propose the creation of collaborative, unclassified Extrapedias in which the expertise necessary to solve problems and monitor events, from border management to scientific research, may be collected in secure collaborative repositories open to vetted contributors in and outside of government*.

### *5.4: Wiretapping*

Although the continuing struggle to combat terror groups and other nonstate threats to the United States requires every intelligence tool possible, the effort to monitor the Internet and other digital telecommunications will continue to require balance. The Foreign Intelligence Surveillance Act was written in a time, not long ago, when international communication was exceptional, not ubiquitous. The warrantless wiretapping controversy has largely abated. However, without compromising sources or methods, it is important for the next administration to issue clear, unambiguous, and unclassified policy regarding the use of digital surveillance technologies to secure American lives, property, and interests at home and abroad. While it is essential to watch the Web and spot those who would do us harm, it is equally essential to monitor the Web and protect it from those who would do it harm. *The administration should consider the publication of an executive-level directive regarding U.S. intelligence policy and the Internet in which it admits that digital surveillance is conducted and that the product of that surveillance is used in a lawful manner.*

## Conclusion

While this set of suggestions is by no means exhaustive, the clear message is that IT matters. A national energy policy is of vital importance and should receive great attention and consideration, but it should not be implemented at the expense of IT. Instead, we should ask how America's information edge may be utilized in a broader technology strategy. Whether in energy, national security, or health policy, IT will be an important—if not the most important—tool available for framing problems and bringing together the expertise necessary to solve them.