

Eight Imperatives

for Leaders in a Networked World:

[A Series of Guideline Papers for the Year 2000 and Beyond]



Imperative 5: Protect Privacy and Security



THE HARVARD POLICY GROUP
ON NETWORK-ENABLED SERVICES AND GOVERNMENT
JOHN F. KENNEDY SCHOOL OF GOVERNMENT

CONTENTS

Preface	i
Disruptive Changes and Tradeoffs in a World of Pervasive Networks	2
What to Avoid: Getting Blindsided on the Road to E-Services	3
What to Do: Push for Transparency and Well-Balanced Progress	4
Guidelines for Protecting Privacy and Security	6
1. Adopt existing practices and standards where appropriate	6
2. Educate and involve stakeholders in exploring and assessing privacy and security	7
3. Give adequate executive-level attention to information policy issues	9
4. Plan for privacy and security before collecting data and/or building systems	10
5. Look to harmonize information policy with other jurisdictions	11
6. Support the development of new technologies and techniques	12
7. Use IT to enhance privacy and security, not just maintain them	13
Next steps	15
Appendices	
A. Membership of the Harvard Policy Group	17
B. Reading and Resources	19
C. Glossary	20
End Notes	24

LIST OF FIGURES

Figure 1. Possible Impacts of Electronic Services on Different Values	5
Figure 2. Guidelines for Protecting Privacy and Security	14
Figure 3. Advice for Stakeholders	16

Overview

“The time is ripe for **public leaders** to engage information **technology** issues more deeply, directly, and successfully.”

PREFACE

As we enter the new millennium, everyone from futurists to the general public has observed that information technologies are changing our patterns of social, commercial, and political interactions. These changes raise profound opportunities and threats for people everywhere. It is a revolutionary period, with many issues not yet fully understood, let alone resolved.

Throughout this period, our public leaders—including elected and appointed officials and their overseers in all branches of government—have too often ignored technology issues or have delegated them to others. The conventional wisdom has been that technology is either not very important, or requires technical expertise rather than leadership, or is simply too risky for leaders to get personally involved.

These views are changing, however. Due primarily to the astonishing growth of the Internet and e-commerce, technology is now widely acknowledged as a critical force in shaping the future. The need for skillful and committed leadership has become obvious.

But the risks are still there.

As a result, public leaders—often under enormous and competing pressures—remain uncertain about how to successfully engage technology-related issues.

In response to these developments, Harvard University’s John F. Kennedy School of Government assembled a group of distinguished public leaders to explore what was being learned about computer networking and its impacts on the roles and responsibilities of government.

The Harvard Policy Group on Network-Enabled Services and Government (HPG) includes legislative and executive leaders, private-sector and public-sector leaders, technology managers and general managers, and public officials from federal, state, and local governments in the United States and Canada. Working over a three-year period, the HPG concludes that the time is ripe for public leaders to engage information technology issues more deeply, directly, and successfully. To improve the quality of engagement, the HPG has developed a set of eight imperatives for those who seek to lead in this critical period. Each of the individual imperatives addresses a significant leadership responsibility and is the subject of a separate paper (for a list of the papers, see the back page). Taken together, the HPG papers provide a framework to guide those who seek to develop successful information age leadership strategies.

The report you are reading explores imperative #5: *Protect privacy and security*. It describes how leaders should approach the privacy and security impacts of electronic services in the context of other concerns such as access, efficiency, and equity. It emphasizes the need for a transparently fair and considered policy-making process that seeks common ground where possible, but makes difficult decisions when necessary. It is clear that the terrorist attacks of September 11, 2001, are motivating new policies and investments to make systems and society more secure. The urgent need for action creates an equally urgent need for insightful analysis and understanding of the interrelated impacts and the many gains and losses made newly possible with the design and delivery of electronic services.

The HPG was made possible through a partnership among the Kennedy School of Government, American Management Systems, Cisco Systems, EDS, IBM's Institute for Electronic Government, the MITRE Corporation, and Unisys. The views in these papers are those of the individual members of the HPG and not the institutional views of their home organizations or project sponsors. However, it would have been impossible for the group to learn and to produce what it has without the opportunity provided by this partnership to meet together and to share insights over an extended period of time.

We sincerely hope that these papers will prove helpful to public and private-sector leaders and to the public at large.

THE HARVARD POLICY GROUP ON NETWORK-ENABLED SERVICES AND GOVERNMENT
CAMBRIDGE, MASSACHUSETTS
DECEMBER 2001

JERRY MECHLING, JOHN F. KENNEDY SCHOOL OF GOVERNMENT
LYNDA APPELEGATE, HARVARD BUSINESS SCHOOL



Technological advances like computer networks have the potential to either support or erode our values. While our future depends, in large measure, on our technological capabilities, it depends even more on how we apply them. Consider the following fictional scenarios:

- As an ambulance rushes an unconscious patient to the hospital, doctors prepare to save him by accessing an online database with data on his pre-existing heart condition. During the same month, people with similar heart conditions are denied jobs when prospective employers gain access to a similar database.
- Taking a break from his job, a computer technician hacks into a local government database that holds the credit card numbers of citizens who paid parking tickets online. In the next town, where citizens cannot pay tickets online, a computer technician spends 40 minutes of her lunch hour waiting in line at city hall to pay a parking ticket.
- In response to a terrorist bombing, a town installs video monitors and face-matching technology as a deterrent; subsequently the public feels safer and terrorist incidents diminish. In a similar town, similar technologies fail to catch terrorists, but usage is expanded greatly as a tool to combat a variety of less serious offenses such as car thefts and pick pocketing.

Whatever you think about the above scenarios, it is clear that computer networks are redefining what information can be collected and who can get access to it. In response, governments are being forced to reexamine their information management policies.

Most government information management policies have focused on data about individuals. Over the years, governments have established rules, standards, procedures, and policies for how information can be collected, analyzed, stored, shared, and discarded. These rules have been created to promote values such as access, efficiency, equity, privacy, and security.¹

As paper-based processes now give way to IT-based processes, the fundamental challenge remains the same: how to promote values that are sometimes in competition. The difference today is that enormous volumes of information can now be collected, used, reused, combined, recombined, and shared instantly and over large distances. While the new information capabilities can be used for dramatically more efficient, convenient, and, in some cases, life-saving services—an obviously positive outcome—they can also be used in ways that challenge traditional assumptions about how to assess and balance different interests and values.

In the first four of our “Eight Imperatives for Leaders in a Networked World,” we focused on how IT is shaping government service delivery—what we refer to as the “e-government” agenda. This report begins our exploration of the final four imperatives—the “e-governance”

agenda. The issues here are more controversial and less clear, and significant influence flows from outside the jurisdictional boundaries of the governments involved. The e-governance agenda is generally less understood than the e-government agenda, and is less likely to offer progress through consensus-supported incremental change.

In this initial paper of our e-governance sequence, we focus how to protect privacy and security in a world of e-services.

“... how can we **govern** the new technology-enabled patterns of human **interaction** while preserving or even augmenting the values we hold dear?”

DISRUPTIVE CHANGES AND TRADEOFFS IN A WORLD OF PERVASIVE NETWORKS

Human interactions inevitably generate conflict as well as cooperation. The role of governance is to resolve such conflicts so as to define and protect the public interest. Wise governance promotes the values held by individuals and groups within society, making tradeoffs that favor one over the other when necessary to advance the greater good of society as a whole.

New information technologies are generating new patterns of human interaction. These new patterns are forcing us to reconsider how we assess and balance many critically important values.

Such challenges are clearly evident in the health care industry. New technologies can give health care workers timely access to patient files so as to improve service and save lives. Hospitals can use similar records to speed reimbursements while reducing administrative costs and errors. Insurance companies can likewise process claims more efficiently while simultaneously reducing fraud. On the other hand, these same technologies can give employers inappropriate access to the health records of prospective employees, or give marketers inappropriate access to lists of potential consumers. Electronic records are also vulnerable to large-scale destruction and misuse both inside and outside the health care system.

In designing Information Age health services then, special care must be taken to balance the values and interests of various stakeholders. What should be the rights and responsibilities of health care consumers versus health care producers? Of health care consumers and producers versus government regulators? Of individuals versus the various groups to which they belong? How should we measure and—when necessary—trade off access versus efficiency versus equity versus privacy versus security?

In some cases, privacy and security are clearly in competition. To protect security we authenticate individual identities, confirm in advance that these individuals are authorized

to take the type of actions they propose to take, and maintain records to hold individuals accountable for their actions after the fact. These steps to preserve security reduce the scope of anonymity that has traditionally been an important protector of privacy.

What even this cursory look at the health care system illustrates is the need to learn how information technology will affect the balance among different stakeholder interests and values. It is clear that ignoring the interrelated impacts of IT risks leads to severely undesirable outcomes. Similarly, focusing on one stakeholder group or value to the exclusion of others will be a mistake. We clearly want to stay alert to possibilities for win-win improvements, where smart choices can create value without a need for agonizing tradeoffs. If anonymity protects individual freedoms but is risky to community security, might we protect those same freedoms by using IT to make government transparent and accountable and avoid most of anonymity's downside risks? The broad and fundamental question is, how can we govern the new technology-enabled patterns of human interaction while preserving or even augmenting the values we hold dear?

Unfortunately, the issues involved are too uncertain and contentious to yield answers that are both simple and useful. The changes under way are so continuously disruptive that answers that may appear to work today will likely have become outdated by the time this report is made public.

The analysis in this paper is weighted heavily towards issues of privacy and tradeoffs between privacy and other elements of information policy. The majority of this paper was compiled before September 11, 2001, and therefore many of the issues being raised in response to the events of that day are not covered here in depth.

So, instead of answers, what we offer here is a framework for analyzing the effects of information technologies on different values and stakeholders. Drawing heavily on recent experience in many governments, we build on this framework to provide guidelines for addressing privacy and security in a networked world.

“In **combination**, these conditions create potentially **devastating threats** to privacy and security.”

WHAT TO AVOID: GETTING BLINDSIDED ON THE ROAD TO E-SERVICES

As the Information Age progresses, the pressure to deliver services electronically is growing. The unit costs of face-to-face service can often be cut by as much as 90 percent when offered on a self-service basis over networks.² From an efficiency standpoint, access to information across organizational, physical, and temporal boundaries can be hugely beneficial.

In the rush for efficiency, however, other values can be overlooked. These can surface later—often negatively—as “unintended consequences.” Early mistakes with electronic services can produce an opposition that makes further progress impossible or may lock government into inefficient systems on a long-term basis.

Privacy and security have emerged as two of the most difficult information-related issues. In part, this is because:

- *They have often been considered secondary concerns for the designers of e-government services—at least until recently.* Many government managers have focused on efficiency and customer satisfaction while considering privacy and security as someone else’s problem.
- *Stakeholders tend towards strongly-held, polarized positions.* This makes compromise difficult and slow to arrive at. Stakeholders have rarely been pulled together for realistic exploration and assessment of options and tradeoffs, although recent terrorist activities are forcing reassessments and will lead to new responses.
- *Governments tend to build large, interconnected systems with multiple components.* Understanding the downstream impacts of different design choices is challenging and complex. Furthermore, once the systems have been built it is difficult to “graft on” privacy and security protections on an after-the-fact basis.
- *Privacy and security are subject to more than government actions and policies.* In a networked world, privacy and security are affected by third parties both known and unknown to government officials, including telecommunications companies and public and private service delivery partners.

In combination, these conditions create potentially devastating threats to privacy and security. In the rush to deliver e-services, it is all too easy to get blindsided and blown off the road.

“We need help in **understanding** what is possible,
in clarifying our values, and **resolving** our conflicts”

WHAT TO DO: PUSH FOR TRANSPARENCY AND WELL-BALANCED PROGRESS

Much is at stake as information technologies continue to evolve. While connectivity and information density should eventually improve service productivity and access—perhaps enormously—significant impacts on equity, privacy, security, and other important values are also likely. As electronic services become more prevalent, it will be critical to understand how different stakeholders and values are being influenced. It will be equally important to

make decisions in a manner that is broadly understood and seen as legitimate. Figure 1 outlines some of the more significant concerns and possibilities.

How can we secure the positives and avoid the negatives?

VALUE	Possible Positive Impacts	Possible Negative Impacts
Access	<ul style="list-style-type: none"> Anytime, anywhere access 	<ul style="list-style-type: none"> Unauthorized, undetectable access
Efficiency	<ul style="list-style-type: none"> Reduced unit costs through self-service, economies of scale, etc. 	<ul style="list-style-type: none"> Rigidities through improper automation of the status quo
Equity	<ul style="list-style-type: none"> More low-cost services 	<ul style="list-style-type: none"> An aggravated “digital divide”
Privacy	<ul style="list-style-type: none"> Context-appropriate access tools Context-appropriate anonymity 	<ul style="list-style-type: none"> Loss of privacy through record linkages Big Brother knows all
Security	<ul style="list-style-type: none"> Better access tools Better audit trails 	<ul style="list-style-type: none"> Vulnerable to interdependencies and uncontrolled access
Other	<ul style="list-style-type: none"> More transparent government 	<ul style="list-style-type: none"> Market domination that improperly erodes “the commons”

Figure 1: Possible Impacts of Electronic Services on Different Values

Advancing successfully will require careful navigation. It will be difficult to secure the positives while avoiding the negatives. The issues to be reconciled are powerful and—at least so far—relatively unstable. Different people are concerned about different values and issues, or in different ways at different times.

While too narrow a focus on any one element is likely to lead to bad results, so is sticking too long with the status quo. For example, we clearly need the service efficiency that could come with information-age health care. However, if electronic services produce overly easy or uncontrolled access to health care information, patients may refuse to talk candidly to their doctors; as a result, both efficiency and privacy could be lost.³ At another extreme, if health-care focuses too much on privacy, emergency room doctors may not get access to crucial information about the patients they are treating, and as a result efficiency (not to mention lives) could also be lost.

Good decisions will depend on good leadership. We need help in understanding what is possible, in clarifying our values, in uncovering win-win opportunities, and in resolving our conflicts. Fundamentally, we need to push for progress that strikes broadly supported and wise choices among competing concerns.

Wisdom

“... allow diverse stakeholders to **understand** the wisdom of the **decisions** and the fairness of the process.”

GUIDELINES FOR PROTECTING PRIVACY AND SECURITY

In responding to privacy, security, and related challenges, leaders need to push for transparency and well-balanced progress. But how can you make this advice operational? Consider the following seven guidelines.

1. Adopt existing practices and standards where appropriate.

Problem. While new technologies highlight new issues, many previously identified practices have yet to be widely adopted. For many governments, a path to significant improvement in privacy and security has been well-charted but not well-traveled.

What to avoid. Do not fall behind through ignorance of constitutional guidelines, laws, regulations, or the experience of others. At the same time, do not adopt externally generated guidelines without carefully considering your own context. Some “good” practices are out of date.

What to do. Explore and—where relevant—adopt or adapt principles and practices that have been validated as good ways to address privacy, security, and other information concerns. Talk regularly with peers to ensure you stay current. Practices and standards are often based on strong historic precedents such as Fourth Amendment protections against unreasonable searches and seizure,⁴ but continue to emerge and evolve.

An Example. The Five Goals of Security. While different authors use different terms, five goals are broadly accepted as critical for information security:⁵

1. **Availability:** Timely and reliable access to data and services.
2. **Confidentiality:** Access available only to intended users.
3. **Authentication:** Confirmation that a person is who they claim to be or—more generally—that a statement claimed to be true is in fact true.
4. **Integrity:** Data protected against unauthorized modification or destruction.
5. **Non-repudiation:** Proof that an action (viewing a file, sending an email) occurred and that identifiable users were party to the action.

Technologies continue to change, but the above goals remain critical. Some security practices—such as training employees to manage their passwords properly—are powerful and relatively easy to implement, yet still widely ignored.

An Example. The U.S. Code of Fair Information Practices. Developed by an advisory committee in 1973,⁶ the five principles articulated in the U.S. Code of Fair Information Practices have been reflected in subsequent guidelines such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the EU Directive on Data Protection. Some have argued that technological changes have made these principles obsolete.⁷ Nevertheless, it is important to understand them before deciding on your own policies. The five principles are:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for individuals to find out what information is being kept about themselves and how it is used.
3. There must be a way for individuals to prevent information obtained for one purpose from being used for other purposes without their consent.
4. There must be a way for individuals to correct or amend records of identifiable information about themselves.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended uses and must take precautions to prevent misuses.

An Example. Drafting and Communicating Privacy Policies. Despite the attention being given to information policy, separate studies by Brown University and the Civic Resource Group revealed that most local, state, and federal websites did not post privacy or security policies.⁸ A December 2000 study by the National Electronic Commerce Coordinating Council (NECCC) came to a similar conclusion, finding a surprising lack of privacy statements on state and local government websites.⁹ In recommending good privacy practices, the NECCC study identified Iowa, Virginia, Maine, Utah, and Idaho as jurisdictions with noteworthy policies that answered four key questions that citizens tend to ask, namely:

1. What information is collected about me?
2. Is the information accurate?
3. How is the information used?
4. Is the information I provide shared with other parties and if so, with whom?

2. Educate and involve stakeholders in exploring and assessing privacy and security.

Problem. As relationships change among information access, efficiency, equity, privacy, and security, it is difficult to keep up with and understand what is possible. Recognizing and developing shared interests is a challenge when stakeholders rarely work together. It is hard to put the puzzle together when the pieces are not on the same table.

What to avoid. Do not expect easy consensus on information issues; progress will likely require firm decisions in the face of ongoing opposition. At the same time, do not run roughshod over minority views; people need time to become convinced that tradeoffs are being made carefully and fairly.

What to do. Speak to stakeholders separately but also bring them together in the design process. While disaster stories and crises may be useful to get attention, be sure to share and analyze realistic cost/benefit and risk data in exploring tradeoffs. Get leaders involved in pilot projects—nothing educates like first-hand experience.

An Example. Record Linkage in Canada. In 2000, Canada's Privacy Commissioner revealed that the federal government had constructed a database on more than 33 million people that linked information from multiple agencies. While the database was not secret and served many valuable purposes—including research and program analysis—it was immediately denounced as an “Orwellian” abuse of power and eventually destroyed. Recognizing that the benefits of record linkage could be lost if public sentiment focused solely on potential abuses, Ivan Fellegi—a pioneer in linkage research—has advocated for a broad and open discussion of responsible data stewardship. By bringing together stakeholders, including the general public, Fellegi seeks to explore the risks and rewards of record linking in an open, transparent, and responsible environment, thereby hoping to avoid situations like the one in Canada.¹⁰

An Example. Difficulties in Consolidating State Computer Operations in Wisconsin. When Wisconsin Governor Scott McCallum proposed allocating \$132.4 million to establish a Department of Electronic Government, privacy advocates highlighted the abuses that might result if a single agency controlled all data without effective safeguards in place. In response, the Governor agreed to work with stakeholders to minimize risks to personal privacy, establishing a Privacy Information Officer with the ability to sue the state or its agencies over privacy-related matters. Underscoring the difficulty of gaining a sustained consensus on these issues, the Joint Committee on Finance later approved the Department of Electronic Government but not the Privacy Information Officer.¹¹

An Example. U.S. Department of Health and Human Services. In 1996, the U.S. Congress passed the Health Insurance Portability and Accountability Act (HIPAA) requiring the Department of Health and Human Services (HHS) to establish standards—including a unique health identifier for individuals—for exchanging and analyzing administrative and financial health care information. Realizing the potential implications of such an identifier, HHS decided not to engage in traditional rule making—i.e. issuing a proposed rule, accepting comments, then issuing a final rule. Instead, they held extensive public hearings to explore the issues in greater depth. After these hearings, HHS determined that—until comprehensive privacy legislation is in place—the risks are too great to proceed with a unique health identifier.

For more information about related HHS decisions, see the “Statement for the Record on a National ID Card” given by HHS before the House Committee on Government Reform and Oversight. www.hhs.gov/asl/testify/t980917a.html

3. Give adequate executive-level attention to information policy issues.

Problem. Privacy, security, and other information policy issues have often been seen as something to delegate to project managers and specialists. This has given these issues lower priority and narrower attention than they deserve.

What to avoid. As information issues develop a higher profile, leaders are beginning to take notice. However, it is not enough merely to delegate these issues to one or more senior-level managers “in addition to your other duties.”

What to do. Information policy—which seeks the right balance among access, efficiency, equity, privacy, security, and other values—requires substantial and sustained attention at senior levels of the organization. Like it or not, the chief executive must “own” the ultimate decisions to be made.

An Example. The Advent of the Chief Privacy Officer (CPO). Realizing the importance of information policy, organizations around the world are beginning to appoint capable executives to high-level information policy positions. For example, in 2000 IBM appointed Harriet Pearson to such a position in order to unify the privacy aspects of its business. Similarly, at the U.S. Internal Revenue Service, Privacy Advocate Peggy Irving is no longer buried in the Information Systems division but now reports directly to the Commissioner. In 2001, the State of Utah became one of the first states to appoint an independent Chief Privacy Officer. Beyond privacy alone, the State of Iowa has appointed senior-level executives for privacy and other executives for security and access to records.¹²

An Example. Enterprise-wide Information Security Officers. While many organizations have traditionally employed information security officers (ISOs), in 2000, New York State became one of the first U.S. states to establish a central office to coordinate security on an enterprise-wide basis.¹³ In 2001, the Texas legislature approved \$600,000 to establish an information technology security office in response to an independent study highlighting security problems. Texas hopes that an enterprise-wide security office will deal with security on a more proactive and effective basis.¹⁴

An Example. New York State’s Committee on Open Government. Responsible for overseeing the state’s Freedom of Information Law, Open Meetings Law, and Personal Privacy Protection Law, New York State’s Committee on Open Government must balance many competing interests. While the Committee is primarily advisory in nature, it exerts considerable influence on information access and privacy by furnishing the Governor and Legislature with a public annual report.

For more information about New York State's Committee on Open Government, visit www.dos.state.ny.us/coog/coogwww.html.

4. Plan for privacy and security before collecting data and/or building systems.

Problem. Government information systems and business processes are difficult to change once established. Retrofitting systems for privacy, security, and/or other concerns is therefore extremely expensive.

What to avoid. Do not assume that you can “work out the kinks” in privacy and security at the end of the development process.

What to do. Build privacy and security into the design of electronic services from the beginning. Engage a diverse array of leaders in early privacy and security reviews. Understand competing values as fully and as fairly and as early as possible.

An Example. Privacy Impact Assessments. A Privacy Impact Assessment (PIA) is a process for evaluating how a system can meet privacy standards before, during, and after development. Much like an Environmental Impact Assessment, some governments are requiring PIAs before approving new projects. The U.S. CIO Council has highlighted the PIA of the Internal Revenue Service as a “best practice.” The Government of Ontario, Canada, also requires a PIA prior to approving projects that may affect client privacy.

For more information about the IRS Privacy Impact Assessment, see cio.gov/docs/IRS.htm
For more information about Ontario's Privacy Impact Assessment, see www.gov.on.ca/MBS/english/fip/pia

An Example. Privacy and Public Access to Electronic Case Files Subcommittee. The purpose of the U.S. federal judiciary's Case Management/Electronic Case Files (CM/ECF) project is to support electronic filing and management of court documents. Recognizing the privacy, access, and security issues, the Judicial Conference of the United States—the policy-making arm of the U.S. Courts—formed a subcommittee to solicit opinions. Combining face-to-face hearings with web-based submissions, the subcommittee has heard from more than 240 individuals and organizations. As subcommittee chair Judge John W. Lungstrum notes, “The Judiciary faces a sensitive and very important policy decision, and it believes that the decision should be based on as wide ranging and open a process as possible.”¹⁵

For more information about the Subcommittee, visit www.privacy.uscourts.gov

An Example. Planning for Security at NASA. The U.S. National Aeronautics and Space Administration (NASA) has separate e-procurement systems for medium and large contracts. Recognizing that the security needs for these systems would differ, NASA dedicated time during the design process to address the security goals for each. As a result, the Electronic Procurement System (EPRO) for larger procurements has additional security solutions

including digital signatures for authentication, identification, and non-repudiation.¹⁶ As the CIO Council notes:

“Government organizations are beginning to recognize the importance of including security considerations in up-front planning for web-based information services. One cannot simply make a priori decisions about security requirements; each service should be examined on an individual basis. The most important first step is to create a security plan. The purpose of the plan is to analyze what can go wrong and to determine responses that reduce the likelihood and consequences to an acceptable level.”¹⁷

5. Look to harmonize information policy with other jurisdictions.

Problem. As networks enable cross-boundary information flows, privacy, security, and other issues are increasingly cross-boundary issues. Analysis and governance must respond to these cross-boundary developments.

What to avoid. Do not act locally on information issues without thinking globally and in the longer-term. You may miss the most important elements of a good solution.

What to do. Look to participate in multi-jurisdictional and public-private forums for political mobilization, standard setting, and best practice development. While governance will always involve governments, industry and other groups must also be recognized as powerful and legitimate stakeholders.

An Example. The U.S./Canadian Public Key Infrastructure Liaison Group. The governments of Canada and the United States are each employing public key technology to build a trusted open network environment for transacting business electronically with private companies, members of the public, and other governments. To explore collaboration, the two countries established a Public Key Infrastructure (PKI) Liaison Group between their respective federal governments. This group shares information on PKI matters and looks for opportunities for collaboration.

For more information about the Liaison Group, see www.cio.gov/fpkisc/US-Canada/index.htm

An Example. Privacy in Europe and the United States. The European Union has worked to harmonize information policy laws throughout Europe. For example, the EU Directive on Data Protection that took effect in October 1998 is designed to harmonize the privacy laws of member countries. Such harmonization stands in contrast to the conflicts between the EU and the United States on privacy issues. While the “safe harbor” provision has created an uneasy truce that is allowing commercial flows to continue without massive interruptions, the EU, the U.S., and other governments will need to collaborate with diverse stakeholders to find long-term solutions to a variety of cross-border information issues.

An Example. The Privacy Diagnostic Tool. Developed in partnership with the Ontario Information and Privacy Commissioner, PricewaterhouseCoopers, and Guardent, the Privacy Diagnostic Tool (PDT) is a self-assessment program used to help organizations gauge their privacy readiness. Using internationally recognized privacy standards, the PDT software outlines ten principles based on fair information practices and asks the user a series of yes/no questions to assess their level of compliance.

For more information about the PDT, visit www.ipc.on.ca

6. Support the development of new technologies and techniques.

Problem. While industry-developed technologies and techniques will continue to shape privacy, security, and related issues, the private sector alone cannot absorb all the risks of development. Without public sector support—including appropriate guidance and regulation—development will miss the mark.

What to avoid. Do not assume that the private sector will develop all needed privacy and security technologies and techniques on their own. On the other hand, avoid isolation from the private sector's enormous potential to develop powerful new innovations.

What to do. Continue to provide public sector support and guidance for fundamental pre-market research. This is perhaps especially true for privacy and security enhancing technologies and for applications related to smart cards, PKI, and networking protocols.

An Example. Using Peer-to-Peer Technology at FedStats.net. Peer-to-peer (P2P) technology is used to share information between computers directly—enabling one computer to search and retrieve information from all others in the same community without the need for storing the information on a large central server. Experimenting with how P2P technology might be used in the public sector, the Federal Interagency Council on Statistical Policy ran a pilot called FedStats.net to link data from multiple sources. Using the pilot, individuals could find and share information on all computers in the defined community. While the security risks of the pilot were minimized by using non-sensitive data, groups at the Defense Advanced Research Projects Agency (DARPA) and elsewhere are now working to make P2P secure enough for many other applications.¹⁸

An Example. Ontario's Use of the Platform for Privacy Preferences (P3P). Developed by the World Wide Web Consortium (W3C), P3P is a standard to enable users to determine whether a website manages personal data in a manner acceptable to the user. P3P-enabled sites make their information management policies available so web browsers can compare a site's policies against the user's preferences, thus allowing the user to make an informed decision on whether to visit the site. While the W3C is an organization dominated by its private sector members, Ontario's Privacy Commissioner is also active in the W3C, helping ensure that public sector interests are well represented.¹⁹

To learn more about P3P, including a list of P3P-compliant sites, visit www.w3.org/P3P

*An Example. **Cryptography, Anonymizers, and Infomediaries.*** The idea that technology infringes on security and privacy is popular but only partially accurate. Technologies can also enhance security and privacy. For example, there is a substantial market for the cryptography that secures data in storage and in transmission. Similarly, there is a growing market to provide anonymous web-browsing and emailing services. Database technology makes it possible for infomediaries to aggregate the data of individual consumers in order to serve as their agents in marketing their personal data or in protecting such data from disclosure.²⁰ The public sector can often play an important role in helping these entrepreneurial markets develop.

7. Use IT to enhance privacy and security, not just maintain them.

Problem. With all the concern about technological threats to privacy and security, the potential of IT to improve privacy and security gets scant attention.

What to avoid. Do not use technology merely to automate old paper-based processes, and do not settle simply for solutions that do no harm.

What to do. Aggressively develop new IT capabilities to enhance privacy, security, access, and other values.

*An Example. **Internal Revenue Service Form 4506.*** When someone wishes to purchase real estate in the United States they usually sign IRS Form 4506, giving the mortgage company access to their tax records as part of the mortgage approval process. The old paper-based version of this form gave mortgage companies access to more than 200 pieces of information, did not explicitly restrict them from selling this data, and was not dated. But when the IRS created an electronic 4506 form, the Privacy Impact Assessment process was used to correct for these concerns. The electronic form thus limits access to the 26 data elements actually required for mortgage review, limits the rights of mortgage companies in disclosing this information, and dates the form to allow for eventual expiry. Electronic services offer many such opportunities to protect privacy and security much better than before.

*An Example. **Property Assessments in Allegheny County.*** In most counties in the United States, property assessment information, complete with the names and addresses of property owners, is public information. The goal was to allow the public to ensure that no one receives favorable treatment. When Allegheny County, Pennsylvania, posted a searchable database of property assessment information on their web site, it quickly became one of their most popular services. However, responding to critics who feared that such information could be used to track down intended victims, the county passed an ordinance removing the “owner name” field from the search screen. The public can still search the paper files by name, but they cannot search by name anonymously on the Internet.²¹

• • •

As private and public services move to electronic channels, concerns about privacy and security are difficult to resolve. This is partly due to the rapid pace of technology and other changes and partly due to the depth and diversity of the values involved.

In many cases, the best way forward may be through watchful waiting and persistence in building a consensus. When decisions must be made without consensus, we need to proceed in ways that allow stakeholders to understand the logic and fairness of the process. This will require good leadership as emphasized throughout the Eight Imperatives reports, and an energetic push for transparency and well-balanced progress.

Key guidelines are summarized in Figure 2.

1. Adopt existing practices and standards where appropriate.
2. Educate and involve stakeholders in exploring and assessing privacy and security.
3. Give adequate executive-level attention to information policy issues.
4. Plan for privacy and security before collecting data and/or building systems.
5. Look to harmonize information policy with other jurisdictions.
6. Support the development of new technologies and techniques.
7. Use IT to enhance privacy and security, not just maintain them.

In sum: Push for transparency and well-balanced progress.

Figure 2: Guidelines for Protecting Privacy and Security

Next Steps

“What should **you** do next to protect **privacy** and **security**?”

NEXT STEPS

What should you do next to protect privacy and security?

1. Take stock of how you handle privacy and security today. Before making changes, look at how your institution handles privacy and security today. Who are the responsible parties? What processes are in place to assess privacy and security and other values such as access, efficiency, and equity? Are the issues well understood by policy-makers? Is the policy-making process well understood and respected by stakeholder groups?

2. Plan ahead and get out in front. Be proactive, not reactive—privacy and security are not issues that can be avoided. Establish procedures such as Privacy Impact Assessments to assess and balance values early (and throughout) the development of IT-related systems. Avoid having to handle privacy and security problems on a retrofit basis, as after the fact add-ons are far too expensive both economically and politically.

3. Adopt an outward looking approach. Traditional boundaries between agencies, municipalities, states, and even nations are newly permeable. Governance in a networked world must therefore address the cross-boundary aspects of privacy and security. Even more than before, think globally and act locally.

Brief advice for different stakeholders can be found in Figure 3 (next page).

• • •

In the past few years, governments have made great progress in delivering services online. Much of this has been generated on a program-by-program, agency-at-a-time basis. While we need to continue with such program-by-program work, the future agenda will be dominated by work requiring cross-boundary cooperation where jurisdiction is unclear. For example, terrorism and other pressures will clearly demand urgent action. The problems that are emerging will be challenging, to say the least. Good governance will require us to design our options and make our choices in ways that are widely seen as appropriate and fair.

This report has offered guidelines for protecting privacy and security in the context of other and often-competing values. Our next report will examine how information technologies are creating new needs for public-private cooperation on issues of economic development.

The President. The critical technology agenda is now a “cross-boundary” agenda where your leadership—augmented by a newly-created federal CIO—is required for e-government progress that protects privacy and security while also improving access, efficiency, and equity.

Legislators. Some of you may naturally gravitate to issues of accessibility, some to privacy, and some to security. But all should educate your peers and the public on the need for balance, and not just wade in with single-issue advocacy.

Governors. Develop the long-term, bipartisan consensus needed to secure public-private cooperation in the context of the global shift to electronic commerce. Create an open and informed policy environment—your best protection against spur-of-the-moment decisions.

Local government leaders. Delivering services at the local level, you are at the frontlines in balancing values such as privacy, security, and access. Work with other municipalities and with states to coordinate your efforts.

Judges. Integrated criminal justice systems are at the forefront of efforts to balance the rights of society to security against the rights of individuals to privacy. Educate the legal community broadly on e-government issues and share your knowledge.

Budget directors. You are in the driver’s seat for investments in cross-boundary and self-service systems that promote access and efficiency while simultaneously raising concerns about privacy and security; be sure your assessment process is balanced and palpably fair.

Agency and program heads. Accept accountability for addressing privacy and security issues, educating yourself and others on the risks, rewards, and tradeoffs involved. Build steps for addressing privacy and security early into all decision-making processes.

Chief Information Officers. More than anyone else you must educate decision-makers on the risks, rewards, and tradeoffs involved with issues of access, efficiency, privacy, security, and equity. Work with other jurisdictions to identify best practices and standards that enable effective but protected information sharing across boundaries.

Technology community. Your success will rise and fall with that of e-commerce, and e-commerce will rise only when the public trusts that privacy and security issues are appropriately handled. Work within your community to advance best practices and standards.

Associations and interest groups. E-government issues—including privacy and security—require a wise balance of innovation and standardization. Your groups should offer key support and partnerships with government to encourage innovation and set standards.

The press. The public needs to understand and decide its priorities on interrelated issues of access, efficiency, equity, privacy, and security. This requires effective and long-term education that you are well positioned to provide. Go to it.

The public. When it comes to access, efficiency, privacy, security and the relations among them, we cannot have everything, but we can have much more in the future if we make wise choices about how to use new technological capabilities. Educate yourself and participate in the politics of choice.

Figure 3: Advice to Stakeholders for Protecting Privacy and Security

Appendix A

MEMBERSHIP OF THE HARVARD POLICY GROUP
ON NETWORK-ENABLED SERVICES AND GOVERNMENT

Ms. Kathleen Adams	<i>Assistant Deputy Commissioner, Systems, U.S. Social Security Administration</i>
Mr. Reg B. Alcock, M.P.	<i>Member of Parliament, Canadian House of Commons</i>
Mr. Arun Baheti	<i>Director of E-government, State of California</i>
Hon. J. Kenneth Blackwell	<i>Secretary of State, State of Ohio</i>
Mr. Russell Bohart	<i>Director, Health and Welfare Agency Data Center, State of California</i>
Mr. Mark Boyer	<i>Senior Manager / Public Sector, Internet Business Solutions Group, Cisco Systems</i>
Ms. Janet Caldw	<i>Director, Institute for Electronic Government, IBM</i>
Mr. Dennis J. Fischer	<i>Commissioner, Federal Technology Services, General Services Administration</i>
Mr. Thomas M. Fletcher	<i>Associate Director, Program on Strategic Computing and Telecommunications in the Public Sector, John F. Kennedy School of Government</i>
Ms. Michele Grisham	<i>Manager / Public Sector, Internet Business Solutions Group, Cisco Systems</i>
Ms. Nada Harris	<i>Deputy Assistant Secretary, Information Resource Management, U.S. Department of Veterans Affairs</i>
Mr. Jono Hildner	<i>Acting Administrator, Health Division, Oregon Department of Human Services</i>
Ms. Kathleen Hirning	<i>Deputy Director for Information Technology, National Partnership for Reinventing Government</i>
Hon. Scott Howell	<i>State Senator, State of Utah</i>
Mr. Steven W. Jennings	<i>Executive Director, Central Technology Center, Harris County, Texas</i>
Hon. Randy Johnson	<i>Commissioner, Board of Commissioners, Hennepin County, Minnesota</i>
Mr. Paul D. Joseph	<i>Chairman, State and Local Enterprise Solutions Committee, Information Technology Association of America</i>
Mr. William Keller	<i>Deputy Commissioner, Department of Information Technology and Telecommunications, City of New York</i>
Mr. John Kelly	<i>CIO and Director, Government Information Technology Agency, State of Arizona</i>
Mr. William Kilmartin	<i>Vice President, State and Local Solutions, American Management Systems</i>
Mr. Steve Kolodney	<i>Director, Department of Information Services, State of Washington</i>
Hon. Timothy Loewenstein	<i>Chairman, Board of Supervisors, Buffalo County, Nebraska</i>
Dr. Barry Lurie	<i>Managing Principal, Public Administration, Unisys Corporation</i>
Mr. Bruce W. McConnell	<i>Director, International Y2K Cooperation Center; (former) Chief Information Policy and Technology Branch, U.S. Office of Management and Budget</i>
Mr. Randall Murphy	<i>Administrator, Management Services Department of Lake County, State of Illinois</i>
Ms. Jane Smith Patterson	<i>Director, Office of Technology, State of North Carolina</i>
Mr. Will Pelgrin, Esq.	<i>Executive Deputy Commissioner, Office of Technology, State of New York</i>

Mr. Alvin M. Pesachowitz *Chief Information Officer, U.S. Environmental Protection Agency*
 Mr. Howard A. Peters III *Secretary, Department of Human Services, State of Illinois*
 Mr. André N. Pettigrew *Member of Executive Cabinet, State of Colorado*
 Ms. Carolyn T. Purcell *Executive Director, Department of Information Resources, State of Texas*
 Ms. Wendy Rayner *Chief Information Officer, State of New Jersey*
 Mr. Rock Regan *Chief Information Officer, State of Connecticut*
 Mr. Robert Reisner *Vice President, Strategic Planning, U.S. Postal Service*
 Hon. Marlin Schneider *State Representative, State of Wisconsin*
 Mr. Larry J. Singer *Chief Information Officer, State of Georgia*
 Mr. Phil Smith *Director, State Federal Relations, State of Iowa*
 Ms. Anne F. Thomson Reed *Chief Information Officer, U.S. Department of Agriculture*
 Hon. Barbara Todd *Commissioner, Pinellas County, Florida*
 Mr. Richard J. Varn *Chief Information Officer, State of Iowa*
 Hon. J.D. Williams *Controller, State of Idaho*
 Mr. Phillip J. Windley *Chief Information Officer, State of Utah*
 Mr. Terry Wood *Councilman, City of Jacksonville, Florida*
 Mr. Robert J. Woods *Commissioner of Federal Telecommunication Services, U.S. General Services Administration*
 Mr. Gregory Woods *Chief Operating Officer, Student Financial Assistance, U.S. Department of Education*

Note: Organizational affiliations and position titles reflect the professional status of HPG members at the time of their initial association with the group.

PROJECT STAFF AND CONSULTANTS

Mr. Scot Barg
Senior Researcher

Mr. Charles Vincent
Editor

Ms. Elisabeth Dietel
Project Assistant

Mr. Richard Sobel
Privacy Consultant

Ms. Evelyn Goldman
E-Learning Developer

Ms. Susan Saltrick
Executive Producer

Appendix B

READINGS AND RESOURCES

- Camp, L. Jean. *Trust and Risk in Internet Commerce*. Cambridge, MA: MIT Press, 2000.
- Cate, Fred H., and Richard J. Varn. *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance*. 1999.
- Cavoukian, Ann, and Don Tapscott. *Who Knows: Safeguarding Your Privacy in a Networked World*. Toronto: Vintage Canada, 1995.
- Council for Excellence in Government. *E-Government: The Next American Revolution*. Washington D.C.: Council for Excellence in Government, 2001. www.excelgov.org
- Garfinkel, Simson. *Database Nation*. Cambridge, MA: O'Reilly Press, 2001.
- Hammond, John S., Ralph L. Keeny and Howard Raiffa. *Smart Choices: A Practical Guide to Making Better Decisions*. Boston, MA: Harvard Business School Press, 1998.
- Judicial Conference Committee on Court Administration and Case Management. *Report on Privacy and Public Access to Electronic Case Files*. June 2001 www.uscourts.gov/Press_Releases/att81501.pdf
- Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.
- National Electronic Commerce Coordinating Council (NECCC). *Privacy Policies: Are You Prepared. A Guidebook for State and Local Government*. Version III. 2000. www.ec3.org
- Office of the Federal Privacy Commissioner, Australia. *Privacy Issues in the Use of Public Key Infrastructure for Individuals and Possible Guidelines for Handling Privacy Issues in the Use of PKI for Individuals by Commonwealth Agencies*. Consultation Paper. June 2001. www.govonline.gov.au/projects/publickey/PKIprivacy.htm
- United Kingdom Public Records Office. *E-government Policy Framework for Electronic Records Management*. Version 2.0. July 2001. www.e-envoy.gov.uk
- United States Federal CIO Council. *Securing Electronic Government*. Prepared by the Security, Privacy, and Critical Infrastructure Committee. 2001.

The National Association of State Chief Information Officers' (NASCIO) Digital Government Working Team has struck a series of issue teams including a team to explore privacy and personalization and a team to explore security and reliability. For more information, see www.nascio.org/hotIssues/dg/index.cfm.

The Center for Technology in Government has published a number of practical studies on creating and using electronic records including, *Gateways to the Past, Present, and Future: Practical Guides to Secondary Uses of Electronic Records and Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation*. www.ctg.albany.edu/creating-using_e-records.html

Other Links of Interest:

- Electronic Privacy Information Center www.epic.org
- Online Privacy Alliance www.privacyalliance.org
- Coalition for Sensible Public Records www.cspra.org

GLOSSARY

Application Service Provider (ASP)—A third-party organization that provides software-based services to clients from a single location over a wide-area network. Represents an outsourcing option for governments who cannot or do not want to deliver and support enterprise applications. Also referred to as Managed Service Providers (MSP) when the software is both delivered and managed by the third-party organization.

Asynchronous Communication—A communication pattern in which the two (or more) parties involved are not communicating at the same time. Telephone conversations are an example of synchronous communication—both parties must be on the telephone at the same time. An email message is an example of asynchronous communication—one party can send a message and the other can read it hours or days later.

Broadband—A general term for high-volume, multiple-channel telecommunications capacity available via a single medium (e.g. a wire or cable). While narrowband (the equivalent of one telephone voice channel) is adequate for the transmission of text and numerical data, broadband connections allow the efficient and reliable delivery of voice, data, and video over one integrated network. Because multimedia content is seen as vital to businesses and consumers alike, electronic networks are increasingly moving to broadband, which in turn will have important long-term implications for commercial development and civic life.

Database—A set of data structured to support the storage, retrieval, and analysis of information, often custom-designed for specific business applications. Databases are central to information processing since they allow new and more efficient ways of assembling records and organizing work. A key step in developing databases is implementing consistent definitions or standards so that data can be meaningfully shared among users. Examples include standard charts of accounts for financial data, standard methods of coding geographical information, and standard templates for archiving audio and video material. (See also: Standards.)

Digital—Data that has been created, transmitted, or stored as a string of signals coded as “1”s (on) or “0”s (off). Data in digital form (text, numbers, graphics, voice, video, etc.) can be stored and processed by computers and communicated at high speed over electronic networks with complete accuracy and reliability. Exact copies of digital data can be made in which the nth copy is indistinguishable from the original.

E-government—A term commonly used to describe the interaction between government and citizens over the Internet. E-government has evolved rapidly from merely publishing or disseminating government information electronically, to online interactions and transactions between government and citizens. As governments begin to reorganize and integrate their work processes to take advantage of computer networks, e-government may come to define a new or transformed relationship between citizens and government enabled by networks.

Electronic Benefits Transfer (EBT)—Refers to the transfer of government benefits (funds or resources) to individuals through the use of a card technology. Individuals access their benefits through Automated Teller Machines or retail point-of-sale terminals.

Electronic commerce (or e-commerce)—Transactions where money is exchanged for valuable goods and services with either the money and/or the goods and services transported over computer networks.

Encryption—The act of scrambling information into a form called a cipher, usually to keep it from being read or modified by unauthorized parties. This is achieved through the use of algorithmic “keys” that scramble the information at one end and unscramble it at the other. Computer-based encryption can be used both for purposes that society wants to prevent (criminal and terrorist communications) as well as those it wants to support (private and secure social and commercial communications).

Enterprise Application—A software application that is used throughout an organization (or enterprise). For example, payroll systems or resource management systems that are used by multiple departments or an online payment processing application that is used across organizational boundaries are all enterprise applications. Such applications are important for realizing economies of scale and for ensuring information can be shared.

Fast Follower(ship)—In the context of innovation diffusion, a fast follower is one who adopts an innovation shortly after the initial innovator (or first mover), but appreciably before the majority of those who eventually implement the innovation. For a more detailed discussion of innovation diffusion see Everett M. Rogers, *Diffusion of Innovations*, Third Edition. New York: The Free Press, 1983.

Geographic Information System (GIS)—A set of hardware and software tools used to gather, manipulate, and analyze geographically referenced data. GIS are used by many government agencies. For example, transportation departments use GIS to determine the most efficient corridors for highway construction, and housing departments use GIS to help select the best locations for urban renewal projects.

Geographic Positioning System (GPS)—A system that uses satellites and small, portable receivers to determine the physical position of an object or person. Increasingly ubiquitous, GPS are used to track the locations of airplanes, boats, cars, and even individuals to within an accuracy of a few meters.

Hardware—Broadly, the physical components of information technology: computers, peripheral devices such as printers, disks, and scanners, and the cables and switches that link digital networks. The key components of computer hardware are microprocessor chips, which have doubled in productivity every 18 months, as measured by instructions executed per dollar (a phenomenon referred to as Moore's law). (See also: Software.)

HTML—Hypertext markup language. See: World Wide Web.

Information infrastructure—The interdependent capacities and standards for digital communication and data processing (both hardware and software) that support the flow of information, much as a highway infrastructure supports the flow of vehicles. (Hence, the vernacular catchphrase, "Information Superhighway," as a general reference to the interconnected system of computer networks exemplified by the Internet.) The ongoing expansion of this information infrastructure raises vital issues about when and how to establish and refine the technical standards on which it operates, including important related questions about funding, security, privacy, and collective democratic values.

Information technology (IT)—The umbrella term that encompasses the entire field of computer-based information processing: computer equipment, applications and services, telecommunication links and networks, digital databases, and the integrated technical specifications that enable these systems to function interactively. (See also: Information infrastructure.) The rapid development and expansion of these technologies over the last twenty years has ushered in the current historical period widely referred to as the "Information Age" or "Information Revolution," comparable in economic and social magnitude to the Industrial Revolution of the early 19th century. The profound transformations brought about by computer networking have made information processing (rather than industrial manufacturing) the key factor in economic productivity and global commerce, thereby supplanting large segments of the traditional blue-collar labor market with a white-collar force of information or knowledge workers.

Internet—The vast network-of-networks that uses open rather than proprietary standards to support computer-based communications at an incredibly large and efficient worldwide scale. Originally developed by the U.S. Defense Department for use in research in the 1960s, the Internet has become the foundation of our information infrastructure, an ever-expanding universe of network services and applications organized in geographically dispersed rather than centralized form.

Kaizen—Originally defined in Masaaki Imai's book *Kaizen: The Key to Japan's Competitive Success*, *kaizen* refers to a process of continuous improvement through small sustainable steps.

Knowledge-based economy—A term used to describe an economy in which the defining factor of production is knowledge. The 19th century saw the rise of the industrial-based economy in which goods were produced in large industrial manufacturing plants. Today, a growing number of people produce, use, and share knowledge in their day-to-day work. Since information can be expressed digitally, computer networks have enabled the rapid growth of the knowledge-based economy.

Leadership—Any act by an individual member on the behalf of a group, with the intent to get the group to better meet its goals. Leadership for previously known problems relies heavily on authority and technical expertise, while leadership for new or adaptive problems relies on getting the group to confront the inadequacies of its old values and routines, and thereby develop more effective solutions. In general, the challenges of the information age (which involve a high degree of confusion and conflict resolution) call for adaptive leadership.

Lifecycle Costs—The costs of developing, maintaining, operating, and eventually retiring an IT system or application. When budgeting for IT initiatives, stakeholders often focus on development costs, overlooking future costs that can represent a larger percentage of the full lifecycle costs.

Managed (or Management) Service Provider (MSP)—See: Application Service Provider (ASP).

Marginal cost—The cost of the next in a series of products. Typically, first products cost more because of the expenditures required to set up the production process, with the unit cost then falling over time as the volume of activity increases. For most manufactured goods, however, diminishing returns-to-scale eventually cause marginal costs to rise. With information-technology products, by contrast, the dynamics are dramatically different: extremely high set-up costs (hundreds of millions of dollars for some software products) followed by almost zero costs for extra copies and no diminishing returns-to-scale for extremely high production volumes. Pricing policies for information goods are thus markedly different than for traditional industrial goods, and pricing policies in the economy at large are likely to change as the Information Age progresses.

Network—A set of communication paths (or channels) and the points (or nodes) they connect, including switches to determine which channel will be used when more than one is available. Computer networks, like telephone networks, can be thought of as telecommunications highways over which information travels. Networks benefit greatly from economies of scope and scale. Digital networks typically use packet-switching rather than circuit-switching to greatly increase efficiency and throughput. (See also: Switching)

Open-source—Computer programs that are distributed as open-source are distributed along with access to the source code—the program instructions as written by the programmer. Once distributed, the author of the program must allow users to modify the code and redistribute it freely, while users are prohibited from selling the program or any derivative thereof without the accompanying source code. The open-source nature of the program is usually protected by an open-source license such as the GNU General Public License (GPL). The rationale behind open-source is that a larger community of programmers will use, improve, and develop the program.

Pen-based Computer—A computer that the user interacts with via an electronic pen or stylus rather than a keyboard or mouse. Most PDAs (see below) or hand-held computers are pen-based computers.

Personal Digital Assistant (PDA)—A small hand-held computer that can be carried around by an individual, and that is most commonly used for personal management tasks such as storing phone numbers, reading email, or scheduling. As wireless technologies continue to develop, PDAs are also being used to communicate over networks.

Portal (or Internet Portal)—On one level, a gateway or single point of entry through which the user can access related information from a variety of sources. For example, many governments are launching portals as a single point of entry to government information. It is interesting to note, however, that as governments adjust to the concept of a single point of entry, they are beginning to rethink how they interact with constituents. Rather than organizing the user's experience around agency boundaries, they are breaking down these boundaries to organize information and interactions around the user's needs.

Productivity—The ratio of goods produced in relation to the resources expended in production. Increasing living standards largely depend upon increasing productivity. Production processes that use information efficiently will typically be much more productive overall than older industrial production methods. This is the principal driving force behind the commercial, social, and political changes catalyzed by information technologies.

Prototype—A pre-production, functioning model of a system or application. A prototype is generally used for the evaluation of design, performance, or production potential.

Public goods—Goods with impacts that “spill over” beyond those directly involved in buying and selling, thus weakening market forces as the mechanism for efficient resource allocation. Computer-based services have the potential of providing many positive spillovers to the public sector, since the marginal cost of IT production over time is virtually zero. One of the paramount political questions of the Information Age is where to draw the boundary between public and private benefits and, therefore, who should pay.

Scope Creep—The gradual accumulation of new or expanded requirements after a project plan (project scope) has been agreed upon by all parties. Scope creep is a significant risk to implementation success as it increases cost and extends project timelines.

Server—A computer program that provides services to other programs or computers. This term is also used to describe the computer on which such a program operates. In the “client-server” network model, client programs make requests from servers connected to the same network. On the World Wide Web (see below) a browser acts as a client program, making requests for files or other information from web servers. These servers can be located any place in the world that is connected to the Internet.

Share-in-Savings/Revenue—A financing strategy whereby government compensates a private-sector partner with a share of funds saved/raised as a result of the partnership. This financing strategy is commonly used when the private-sector partner agrees to cover the up-front costs of a project. It is also used to align incentives with desired outcomes.

Slow Trigger, Fast Bullet—An analogy used to describe an implementation strategy in which careful project planning and preparation (the slow trigger) is followed by swift and decisive action steps (the fast bullet) that quickly move the project to a stage that safely demonstrates value.

Smart Card—A small electronic device or token (often the size of a credit card) that stores information in a memory chip. Information can be added, read, or changed using a smart card reader.

Software—A catchall term for the sets of instructions (programs) used to operate computer hardware. Software production and maintenance today has become a primary determinant in the success or failure of business and government organizations.

Source Code—See: Open-source.

Standards—In the context of electronics, standardized technical specifications allow functions to be coordinated by automatically adhering to the set standard. Thus, standards for the voltages used for signaling allow devices to “talk to one another” in a consistent format, and standards for financial accounting allow for the meaningful aggregation and analysis of financial databases. With information technologies there is an inherent tension between the creation of new capabilities through innovation (a few people trying new ways to do things) and the subsequent applications of those capabilities through standardization (many people following established ways of doing things). Determining when and how to set standards is therefore a critical leadership issue, as is deciding whether such standards should be “open” for use by the general public or whether they should be protected by copyright or patent statutes.

Switching—The engineering mechanism that designates alternate channels or paths in a telecommunications network. Historically, telephone networks have used circuit-switching, where an entire channel between two connections is made available for the duration of the communication. Most computer networks, by contrast, have been designed to use packet-switching, which breaks up the transmitted data into individual units or “packets,” each of which contains the destination address of the data. The packets are then independently routed through the network and reassembled by the computer at the destination address. Packet-switching allows data from multiple users to efficiently use the same path on the network. Major developments are now underway to enable packet-switched networks to carry digital voice and video more effectively.

Total Quality Management (TQM)—A management philosophy that became popular in the 1980s and 1990s. TQM is focused on continuously improving the performance of all individuals and processes in achieving customer satisfaction.

World Wide Web (www or Web)—Standardized tools and software that allow non-technical users to find, display, and communicate text, graphics, voice, and video located on the Internet. The Web’s fundamental components include HTML (hypertext markup language), pointers or hyperlinks (that rapidly access specific material that may reside on computers halfway around the world), and browsers (software that allows users to display and interact with Web content). Web technology is credited with democratizing the Internet by simplifying and streamlining key networking tools and functions for the general public.

END NOTES

¹The majority of the research and discussion leading to this paper was conducted prior to the terrorist attacks on the World Trade Center of September 11, 2001. Note, then, that this paper refers to security in the context of control over access to information stored on networks and not in the context of personal or national security. This is not a paper primarily about the use of IT to protect IT-related infrastructure, to permit stronger policing and homeland defense, or to detect and disrupt terrorist networks throughout the world. It is rather a paper about how IT-based services designed primarily for efficiency and effectiveness can produce strong impacts on privacy and on security that need to be considered in designing and deploying such services.

²In a research note Gartner Group estimates that a transaction handled by counter tellers at a bank costs between \$1.00 and \$2.00 per transaction, while a similar transaction conducted over the Internet costs between \$.02 and \$.05. Gartner Group, "The Benefits of Alternate Channels in the Branch," May 1999.

³The Canadian Medical Association has recognized this threat and is lobbying the Government of Canada for legislative changes that would limit data mining by drug companies and hospital foundations. See Anonymous, "Canadian doctors raise questions about data mining," *CBC.ca*, 17 August 2001 (cbc.ca/cgi-bin/templates/view.cgi?news/2001/08/15/Consumers/medicalprivacy_010815).

⁴See analysis of the Fourth Amendment at: <http://caselaw.lp.findlaw.com/data/constitution/amendment04/>.

⁵For more detail on the goals of security, see chapter 4 of Jean Camp, *Trust and Risk in Internet Commerce*, Cambridge, MA: MIT Press, 2000 (ksghome.harvard.edu/~jcamp.academic.ksg/trustRisk).

⁶U.S. Department of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers, and the Rights of Citizens," 1973.

⁷For example, see John Gaudin, "The OECD Privacy Principles: can they survive technological change?" *Privacy Law and Policy Reporter*, Australasian Legal Information Institute (www.austlii.edu.au/au/other/plpr/1996/68.html).

⁸See, Darrell M. West, "Assessing E-Government: The Internet, Democracy, and Service Delivery by State and Federal Governments," September 2000 (www.insidepolitics.org/egovtreport00.html); Civic Resource Group, "Cities on the Internet 2001: E-Government Applied," August 2001 (www.civicresource.com).

⁹National Electronic Commerce Coordinating Council, "Privacy Policies: Are You Prepared. A Guidebook for State and Local Government Version III," December 2000.

¹⁰Ivan P. Fellegi, "Record Linkage and Public Policy: A Dynamic Evolution," In Wendy Alvey and Bettye Jamerson (eds), *Record Linkage Techniques, 1997*. Washington D.C.: Federal Committee, 1997. For more on record linkage see also United States General Accounting Office, "Record Linkage and Privacy: Issues in Creating New Federal Research and Statistical Information," April 2001 (GAO-01-126SP).

¹¹Dennis Chaptman, "A question of privacy: Governor welcomes input on plan to consolidate state computer operations," *Milwaukee Journal Sentinel*, 23 April 2001.

¹²Ellen Perlman, "The Privacy Czars," *Governing Magazine*, July 2001.

¹³John Marcotte, "Surfing the Digital Beat," *Government Technology Magazine*, May 2000.

¹⁴Dibya Sarkar, "Texas setting up security office," *Federal Computer Week*, 5 June 2001.

¹⁵Administrative Office of the U.S. Courts, "Judiciary to hold Public Hearing on Internet Access to Court Documents," News Release, 16 February 2001 (www.privacy.uscourts.gov/Press.htm). The final report of the committee, Report on Privacy and Public Access to Electronic Case Files, was released in July 2001 and is available at www.uscourts.gov/Press_Releases/att81501.pdf.

¹⁶CIO Council, Security, Privacy, and Critical Infrastructure Committee, *Securing Electronic Government*, CIO Council, 19 January 2001.

¹⁷CIO Council, Security, Privacy, and Critical Infrastructure Committee, *Securing Electronic Government*, CIO Council, 19 January 2001.

¹⁸Dan Caterinicchia, "Computers with a view: Feds exploit Napster-style technology," *Federal Computer Week*, 14 May 2001.

¹⁹Along with The Center for Democracy and Technology, Ontario's Information and Privacy Commissioner published a report titled "P3P and Privacy: An Update for the Privacy Community." March 2000. The report is available at www.cdt.org/privacy/pet/p3pprivacy.shtml.

²⁰For a more detailed discussion of how technology is reinventing the privacy debate read Toby Lester, "The Reinvention of Privacy," *Atlantic Monthly*, March 2001.

²¹Jeffrey Cohan, "Council votes to hide names on Web site," *post-gazette.com*. 20 June 2001 (www.post-gazette.com/regionstate/20010620countycouncil0620p2.asp).

EIGHT IMPERATIVES FOR LEADERS IN A NETWORKED WORLD
REPORTS IN THE SERIES

Eight Imperatives for Leaders in a Networked World—Overview (March 2000)

- #1 Focus on How IT Can Reshape Work and Public Sector Strategies (December 2000)
- #2 Use IT for Strategic Innovation, Not Simply Tactical Automation (January 2001)
- #3 Utilize Best Practices in Implementing IT Initiatives (March 2001)
- #4 Improve Budgeting and Financing for Promising IT Initiatives (April 2001)
- #5 Protect Privacy and Security (December 2001)
- #6 Form IT-related Partnerships to Stimulate Economic Development
- #7 Use IT to Promote Equal Opportunity and Healthy Communities
- #8 Prepare for Digital Democracy

FOR MORE INFORMATION ON ORDERING COPIES OF THESE REPORTS:

www: <http://www.ksg.harvard.edu/stratcom/hpg>

email: 3e_project@ksg.harvard.edu. (Please put “HPG publications” in the subject line.)

mail: E-Government Executive Education Project
John F. Kennedy School of Government, Harvard University
79 JFK Street, MA-124, Suite 195
Cambridge, MA 02138
attn: HPG publications

phone: 617-495-3036

fax: 617-495-8228

The HPG was made possible through a partnership among the Kennedy School of Government, American Management Systems, Cisco Systems, EDS, IBM's Institute for Electronic Government, the MITRE Corporation, and Unisys.



THE HARVARD POLICY GROUP
ON NETWORK-ENABLED SERVICES AND GOVERNMENT
JOHN F. KENNEDY SCHOOL OF GOVERNMENT
CAMBRIDGE, MASSACHUSETTS