E-Government Series

January 2001

Privacy Strategies for Electronic Government

Janine S. Hiller
Center for Global Electronic Commerce
Pamplin College of Business
Virginia Polytechnic Institute and State University

France Bélanger
Center for Global Electronic Commerce
Pamplin College of Business
Virginia Polytechnic Institute and State University

The PricewaterhouseCoopers Endowment for
The Business of Government

The PricewaterhouseCoopers Endowment for

The Business of Government

About The Endowment

Through grants for Research and Thought Leadership Forums, The PricewaterhouseCoopers Endowment for The Business of Government stimulates research and facilitates discussion on new approaches to improving the effectiveness of government at the federal, state, local, and international levels.

Founded in 1998 by PricewaterhouseCoopers, The Endowment is one of the ways that PricewaterhouseCoopers seeks to advance knowledge on how to improve public sector effectiveness. The PricewaterhouseCoopers Endowment focuses on the future of the operation and management of the public sector.

Privacy Strategies for Electronic Government

Janine S. Hiller
Center for Global Electronic Commerce
Pamplin College of Business
Virginia Polytechnic Institute and State University

France Bélanger
Center for Global Electronic Commerce
Pamplin College of Business
Virginia Polytechnic Institute and State University

January 2001

TABLE OF CONTENTS

Foreword

January 2001

On behalf of The PricewaterhouseCoopers Endowment for The Business of Government, we are pleased to present this report by Janine S. Hiller and France Bélanger, "Privacy Strategies for Electronic Government."

As we witness the astronomical growth of e-commerce in the private and public sector, both businesses and government struggle with public perceptions and concerns about the privacy and security of information on the Internet. The federal government must move quickly to address these concerns. This report provides a framework for understanding the implications of privacy and security in the public domain, the challenges for increasing use of the Internet to deliver services, and the connections and lessons that can be learned from the private sector's experience with privacy and security issues.

Hiller and Bélanger propose an e-government framework that identifies six constituent relationships and five stages of e-government. The combination of relationships and stages of e-government are more complex than in electronic commerce in general. The authors assert that these relationships must be taken into account when the government is considering the level of privacy and concerns about privacy and security by its constituents.

The report presents a series of recommendations to the federal government with respect to privacy in e-government, including: meet the legal requirements to instill confidence and trust in government; gain individual confidence by addressing privacy perceptions; gain the confidence and trust of businesses by encouraging participation in the marketplace and creating efficiencies; and work with state and local governments and agencies to develop standardization and shared privacy standards.

We trust that this report will be helpful to public sector leaders as they seek to expand e-government while protecting the privacy of citizens.

Paul Lawrence
Partner, PricewaterhouseCoopers
Co-Chair, Endowment Advisory Board
paul.lawrence@us.pwcglobal.com

Ian Littman
Partner, PricewaterhouseCoopers
Co-Chair, Endowment Advisory Board
ian.littman@us.pwcglobal.com

Executive Summary

Electronic government spending in the United States is predicted to be in excess of $20 billion during the 2000-2005 period. In particular, electronic government spending for the federal government alone will reach $2.33 billion by 2005. This is more than the expected spending by consumers from retail businesses ($2.24 billion). Despite this growth, businesses and the government are struggling with public perceptions and concerns about the privacy and security of information on the Internet. This report provides a framework for understanding the implications of privacy in the electronic federal government, using the lessons learned from the private sector's experience with privacy issues.

The report discusses data collection practices of the private sector and the resulting privacy concerns of consumers. While legal restrictions do exist, self-regulation by industry leaders is their most visible response to consumers' privacy concerns. This attempt at self-regulation has mostly taken the form of trust seals, such as TRUSTe, BBBonline, and CPA WebTrust.

An electronic government (e-government) framework is presented, which depicts the complex relationship that exists between types and stages of e-government. The five stages of e-government include information, two-way communication, transaction, integration, and participation. As government evolves through these stages, data collection and related privacy concerns increase for all types of e-government. The types of e-government include:

- government delivering services to individuals
- government to individuals as part of the political process
- government to business as a citizen
- government to business in the marketplace
- government to employees
- government to government

While the government faces issues relating to the collection of private information similar to those of businesses, it is legally restricted in different ways in its use and sharing of personal information. These differences are reviewed.

The CPA WebTrust is presented in this report as a best practice for privacy standards in business. Comparisons of the WebTrust with the government's best practice (IRS privacy statement) and the Privacy Act reveal that the private sector is a step ahead of the government. For example, federal policies and standards are often found in general language, while the specific language of the WebTrust is more helpful. In addition, federal practices are found in multiple places instead of in a summarized and central document that could be used by all agencies. Based on this comparison and other findings of the research, we make the follow-

ing recommendations to the federal government with respect to privacy in e-government:

1. The government must meet the legal requirements to instill confidence and trust in government.

Recommendation 1A: Make electronically available, in an easy to read and understand format, the intent to exempt records from disclosure under the Freedom of Information Act (FOIA).

Recommendation 1B: Review the business confidential and trade secret information exception to the FOIA for timeliness in the electronic environment.

Recommendation 1C: Make disclosures under the Privacy Act available electronically, in standard and easily readable form.

Recommendation 1D: Consider the collection of Internet Protocol (IP) addresses as "personally identifiable information" under the Privacy Act.

Recommendation 1E: Review the efficiency of Data Protection Boards under the Computer Matching Act.

2. The government must gain individual confidence and trust by addressing privacy perceptions.

Recommendation 2A: Conduct repeated, longitudinal e-government privacy studies.

Recommendation 2B: Create a government privacy seal program and develop standard, precise, and clear privacy statements.

Recommendation 2C: Educate constituents on privacy and security in e-government.

3. The government must gain the confidence and trust of businesses by encouraging participation in the marketplace and creating efficiencies.

4. The federal government must work with state and local governments and agencies to develop standardization and shared privacy standards.

Introduction

Electronic commerce in the private sector is growing by astronomical measures. Estimates vary greatly, but commerce on the Internet has been forecasted to exceed $37 billion in the next three years. In addition, the number of new Internet users increases by 10 percent each month. The combination of these two figures seems to indicate an unstoppable trend. The public sector, both federal and state, will also be increasingly delivering services and distributing information by means of the Internet. Predictions are that citizens will be able to conduct some electronic transactions with more than 60 percent of government agencies in Organisation for Economic Co-operation and Development (OECD) countries by 2003. In addition, predictions put e-government spending in the United States in excess of $20 billion during the 2000-2005 period (Gartner Group, April 2000). In particular, e-government spending for the federal government alone will reach $2.33 billion by 2005. This is more than the expected spending by consumers from retail businesses ($2.24 billion).

Despite this growth, there is an important issue that could reverse or slow the trend. Businesses are struggling with public perceptions and concerns about the privacy and security of information on the Internet. In the absence of regulation by the government, self-regulatory agencies and trust seals have been designed to address the public concern. Public sector services are constrained by more specific privacy restraints, but will face similar issues of privacy and security as they increase access to information and delivery of services electronically.

This report provides a framework for understanding the implications of privacy and security in the public domain, the challenges for increasing use of the Internet to deliver services and information, and the connections and lessons that can be learned from the private sector's experience with privacy and security issues. Privacy and security practices in e-commerce can provide input into the issues of public use of the Internet for e-government. Because of the breadth of the topic, the focus in this report is primarily on the federal government, its use of citizen information, and the concurrent privacy issues faced in the transition to electronic government.

Businesses, Data Collection, and Privacy

Overview of Data Collection Practices

Collection of data about individuals has always invoked issues of privacy. However, online technology increases the concerns as it allows for storage of more data, faster and easier than before. In addition, it allows for easier manipulation of that data and cross-referencing at unbelievable speed (Punch, 2000). Finally, in the online world, data collection can also occur without the knowledge of the individual. Each of these issues is described in more depth below.

Faster and Easier Data Collection

Corporations and organizations collected information about consumers before the advent of the Web. When consumers completed registration cards for warranties, for example, corporations transferred that information into their databases. The information was often used to send unwanted (junk) mail to the users via the postal system. The difference today is that the collection of data can be done faster and easier (and without an individual's knowledge). Current technology allows easy loading of data forms on websites directly into databases. For companies this is a major advantage since the data are loaded immediately (faster) and accurately (no transcribing errors and no problems dealing with unreadable writing). Data are also easier to collect since tools have been developed, such as "cookies," for collecting the information from the users, even information the average user does not know (such as their IP address). Naviant's High Tech Household File reportedly contains information about 17.5 million households that are connected to the Internet, and it increases this number by thousands each month. Engage states that it has information about 53 million households, and DoubleClick claims to have 100 million informational listings. In this election year, Aristotle International claims data on 150 million voters in the United States.

Cross-Referencing (aggregation)

One of the biggest public outcries concerning online privacy happened following the merger of two companies, DoubleClick and Abacus Direct Corp. The former provides Internet network advertising and collects anonymous online purchasing data and browsing habits through cookies (Anstead, 2000). The latter provides specialized consumer data and analysis for direct marketing and has a database of 88 million buyer profiles collected by 1,500 direct marketers and online retailers (Punch, 2000). After the merger the companies announced the decision to merge the two databases. This is also called triangulation (Melillo, 1999). Cross-referencing real offline consumer data with online purchasing habits (collected with or without the individual's knowledge) led privacy advocates to raise serious privacy issues. DoubleClick temporar-

ily stopped their plans to merge the two databases after the public uproar.

The potential for cross-referencing online data with other online data (between several Web entrepreneurs, for example) is another concern of privacy advocates (Melillo, 1999). In 1999, U.S. Bancorp rented customer information, in conflict with its privacy statement. It settled a case brought by the Minnesota Attorney General, but in doing so stated that it was following "industry-wide practice[s]" (Money, 2000). The Toysmart bankruptcy case, involving the proposed sale of personal data as an asset, has also raised concerns. Although Toysmart agreed never to share the information it collected, the data was treated as an asset that could be sold to pay creditors in bankruptcy proceedings. The resolution is not final at the time of this report, but will involve the Federal Trade Commission (FTC) and the Bankruptcy Court positions regarding the sale of the information.

Hidden Data Collection

Besides the issue of cross-referencing data between online and offline databases, collection of data without consent is the biggest issue privacy advocates are raising with online websites. Contrary to the "old days" of warranty card registration, now data can be collected about individuals without their permission or active participation. As users customize their web browsers with personal information, they do not always realize that this information can be accessed from websites they are visiting and then stored in the website's databases. Usually this is accomplished by means of "cookies."

There are four cookie-based ways or strategies to collect consumer information on the Web: association, anonymous data, contest website, and compensation models (Melillo, 1999).

- Association models of data collection match visitors of a website with other visitors with similar buying habits (Amazon.com uses this strategy). This strategy is accomplished through the use of cookies — small data files placed on the user's computer when they first visit a site.
- Anonymous data models follow a consumer's surfing patterns to gather profiles over a number of sites without knowing the individual's name (Engage Technologies collects data this way). This model also uses cookies. It provides what is called "clickstream" data — information about where people go within a site and the ads and content they see (Green et al., 1998). Some models will also follow individuals after they leave the site.
- Contest websites offer chances to win prizes to consumers who register with them. Advertising is then sent to these users. (DoubleClick uses this method.)
- Compensation models offer consumers payment in the form of access or the chance to win a sweepstakes in return for personal data. (Free-PC uses this strategy.)

Benefits of Data Collection

Collection of consumer data raises serious concerns with privacy advocates, as outlined earlier. However, businesses and even consumers also see a positive side to data collection — the possibility of personalization and customization of the consumer's interaction with organizations on the Internet and the more efficient allocation of resources by businesses to meet the needs and desires of the consumer. Consumers will often agree to give personal information on the Web if it means they can get better service and convenience on that particular website (Sweat, 2000). Some of the benefits for consumers include access to reward systems (discounts, coupons, prizes, etc.), time savings (after logging in, all preferences and personal information are automatically available), and convenience (by offering combined services or tailored offers according to the consumer's preferences). A significant issue that some consumers have is with companies that collect data and then resell it to others or use it for excessive marketing.

Consumer Privacy Concerns in Business

There are a great many studies of online privacy concerns and privacy practices of businesses. The Federal Trade Commission has completed two of these studies, in 1998 and 2000, and it has recognized another, the Georgetown Internet Privacy Policy Survey, in 1999. These three studies are

helpful in documenting longitudinal consumer concerns over online privacy and the response of businesses to these concerns. The 1998 FTC survey, which included over 1,400 websites, found that while almost all of the sites collected information, only between 14 percent and 16 percent had any statement or policy regarding information collection or privacy.

A follow-up study conducted in 1999, the Georgetown Internet Privacy Policy Survey, looked at similar characteristics, using a sample of 364 online businesses. The FTC recognized this study in its 1999 report to Congress. The results showed that 92.9 percent of the websites collected at least one identifying type of personal information (e.g., name, e-mail address, or postal address of the Web surfer) while 56.9 percent collected at least one demographic type of information (e.g., gender, geographic area, or preferences), and 56.5 percent of the sites collected both types of information (Punch, 2000). In addition, 65.7 percent of the sites posted information disclosures and 44 percent posted privacy policies.

In 1998, the Online Privacy Alliance (OPA) funded research on online privacy practices by the top 100 dotcoms, which was reported to the Federal Trade Commission as a second part of the Georgetown study. The OPA is a coalition of about 100 companies and associations supporting online consumer privacy self-regulation. The findings of the study indicate that all of the top 100 e-commerce businesses collected at least one type of personal information. Of those, 99 percent collected at least one type of information that could be used to identify Web surfers on their site. In addition, 75 percent collected at least one type of demographic information. Moreover, 74 percent of the top sites collected both personally identifiable and demographic information on their websites (OPA, 1999).

The OPA study also evaluated the privacy disclosures of the top 100 companies on the Internet. They examined two types of disclosures: privacy disclosures where a privacy policy notice is posted on the website, and information practice statements. Privacy policies describe a site's general information practices in a single location accessible through a link, whereas information practice statements describe a site's policy for a particular practice, such as handling of credit card numbers online (Punch, 2000). Ninety-four percent of the sites posted at least one type of privacy disclosure and 60 percent posted both types of disclosures. In comparison, the broader survey of websites (Georgetown study) indicated that 65.7 percent of the sites posted at least one type of privacy disclosure, with 36.3 percent displaying both types. A different study focusing on financial institutions revealed that in 1999 only 48 percent of banks and savings associations' websites posted some type of privacy disclosure, 40 percent posted a privacy policy, 39 percent an information practice statement, and 29 percent posted both types (Punch, 2000).

The FTC 2000 Privacy Survey and the appended Online Profiling report provide the most recent and significant data. In the privacy survey three types of information were collected from websites: 1) Does the website collect personally identifiable information?; 2) Does the website contain policy statements?; and 3) What is the content of those policies? Ninety-nine percent of the most popular websites, and 97 percent of the random sample collected personally identifiable information. Eighty-eight percent of the random sites had some statement about privacy, while 100 percent of the most popular websites had a privacy statement. Clearly, there has been progress made in promoting privacy policies in electronic commerce.

The last part of the FTC analysis, however, produced less satisfying results. Using the four fair information practices long accepted as the standard for privacy — notice, choice, access, and security — the FTC reviewed the websites' policies for inclusion to determine the strength of the policy statements. The results showed that only 42 percent of the most popular websites and 20 percent of the random sample included some aspect of all four fair information principles. In a significant deviation from prior reports, while commending the industry for the strides made in self-regulation, the FTC recommended to Congress that legislation be passed that would require that fair information practices be followed at consumer websites.

In the Online Profiling report to Congress, the FTC noted the *Business Week*/Harris Poll that found that

91 percent of consumers were uncomfortable with profiling across websites. The FTC concluded in its study of online profiling that consumers should be given notice of information collection and a choice about what, how, and with whom their information will be shared.

Limitations on Business Collection and Use of Personal Data

Limitations on business use of personally identifiable data can be categorized into two primary areas: public acceptability and legal restrictions.

Public Acceptability Regarding Privacy

Although public opinion itself cannot mandate limits on the business use of information, it is clear that consumer concern with privacy is having an impact on the consumer Internet market, and that for electronic commerce to reach its full potential, this concern must be addressed. For example, a *Business Week*/Harris poll of 999 consumers in 1998 revealed that privacy was the biggest obstacle preventing them from using websites — above cost, ease of use, and unsolicited marketing (Green et al., 1998).

In an IBM Multi-National Consumer Privacy Survey in 1999, 80 percent of the U.S respondents felt that they had "lost all control over how personal information is collected and used by companies." Seventy-eight percent indicated they had refused to give information because they thought it was inappropriate in the circumstance, and 54 percent had decided not to purchase a product because of a concern over the use of information collected in the transaction. Specifically, 72 percent of U.S. respondents were worried about the collection of information over the Internet. Another study by Forrester Research supports these findings, showing that two-thirds of consumers are worried about protecting personal information online (Branscum, 2000). Finally, one of the most recent surveys of consumer attitudes toward privacy is the Pew Internet & American Life Survey. Sixty-six percent of the respondents believe that online tracking should be outlawed, and 81 percent support rules for online information gathering. An impressive 86 percent believe that businesses should ask (opt-in) before collecting information about them.

Legal Restrictions

Unlike other countries, the United States has no overarching informational privacy law applicable to the private collection of data. Nor does it recognize a general right of privacy that is expressed in other countries as a fundamental human right. Instead, most privacy law was enacted in response to a particular event or a perceived need for a specific industry, and in response to the abuse or potential abuse of the collection and use of data in that industry. The following section briefly explains the primary laws regarding privacy of personally identifiable information in the private sector and the business areas affected.

Financial Services Privacy Act of 1978 and Financial Services Modernization Act (FSMA) of 1999

The Financial Services Privacy Act of 1978 prohibits banks from sharing information about bank accounts with federal or state governments. While this statute protects the privacy of financial information from government, it does not apply to sharing information between businesses. In 1999, the FSMA (also known as the Gramm-Leach-Bliley Act) was passed. The FSMA protects the privacy of consumer information held by financial institutions with regards to non-governmental entities. The statute requires banks and financial services companies to give consumers annual information about privacy policies and notify consumers before their information is sold to unaffiliated entities. Regulations to enforce notification and consumer choice are due to go into effect July 1, 2001, so that institutions have the time to institute proper procedures.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The primary impetus for HIPAA was to decrease the costs of processing federal health benefits by requiring electronic submission. Electronic submission of private health information has serious privacy implications , and the act also included a provision to protect the privacy and security of that information when held and transmitted by health organizations and their business partners. Congress self-imposed a deadline of August 1999 to pass the regulations itself, and after that time the duty to write regulations passed to the Department of Health and Human Services (HHS). As the deadline

passed without congressional action, HHS received comments, and proposed regulations that would assure notice, consent, access, security, and accuracy of personal health information. The final regulations were issued December 20, 2000, and will become effective for most health entities in February 2003.

Electronic Communications Privacy Act (ECPA)
The ECPA was passed after the Watergate scandal in reaction to the electronic eavesdropping and surveillance that was brought to light during that time. It prohibits the interception, disclosure, use, or access of messages without authorization or consent. It also imposes nondisclosure limitations and prohibits monitoring of stored electronic communications by providers. This act applies to both government and private entities and is most relevant in this paper with regards to its limitations on the sharing of e-mail communications.

Child Online Privacy Protection Act (COPPA)
The COPPA is recent legislation aimed directly at the online activities of businesses that market to children or who know that children use their website. The act was passed after the Federal Trade Commission documented the widespread collection of information from children and pursued those businesses that did not follow its stated online privacy policies about that collection. The most visible of those cases is the Liberty Young Investor website. This site was aimed at children through its design, games, and free giveaways. It asked children about how much they received each week in allowance, what kind of car the family drove, gifts, and about family finances. The site did not follow its promise of anonymity but recorded the information in personally identifiable files. A settlement was reached in the case. This and other occurrences led to the adoption of COPPA to protect children from online information collection. The statute applies to collection of information from children under 13, requiring explicit parental approval and prominent notices of privacy practices.

Federal Trade Commission Act
The FTC has a broad grant of power to regulate "unfair or deceptive practices" in commerce. Under this mandate it has traditionally regulated advertising and commercial practices. As in the Liberty Young Investor site example, the FTC will pursue businesses whose websites do not comport with the privacy statements portrayed to the public. There is no reason to think that the FTC will not continue to do so under its general regulatory power. In addition, the FTC is active in the area of privacy and the Internet, has sponsored many studies and workshops on privacy and online profiling, and has recommended to Congress that privacy legislation be adopted.

The Fair Credit Reporting Act
Credit reporting agencies are prohibited from furnishing information to anyone except to those with a legitimate purpose and with the consent of the party. Consumers are entitled to access information collected about them and must be allowed to correct data. Penalties are imposed for improper use of credit reports. The act was passed amidst reports of inaccurate and damaging consumer credit reports and the lack of recourse by the injured parties.

Cable Communications Policy Act
Cable companies may not collect information about their customers without their consent and may not share this information with third parties. Annual notice of policies and procedures must be given to customers. Damages of at least $1,000, punitive damages, attorney's fees, and other costs are awarded for violations.

Video Privacy Protection Act
Businesses may not share information about the videos consumers rent except with their permission, by court order, or for collection of fees. Damages of at least $2,500, punitive damages, attorney's fees, and other costs are awarded for violations. The Supreme Court nomination hearings for Judge Robert Bork highlighted the ease of obtaining lists of videos rented for public disclosure, and this act prohibits their release.

Business Response to Consumer Concerns

Industry heard loud and clear the words of the FTC and the administration regarding the protection of consumer privacy, and accepted the invitation

to take the lead by designing a self-regulatory approach. In addition to domestic pressure for self-regulation, international pressure from the European Data Privacy Directive added to the push for measures and standards for protecting consumer privacy. Some of the actions taken by business have been alluded to in prior sections. First, the business community made a significant effort to make sure that websites post a privacy statement. As the statistics reported show, this was a significant improvement in notifying consumers about information collection. Industry groups, such as the Online Privacy Alliance, were established in order to address the privacy concerns of consumers. In a substantive attempt at self-regulation, several entities took on the goal of providing an industrywide regulatory framework. The primary focus of the self-regulatory groups has been on the creation of trust seals. The major ones include TRUSTe, BBBOnline, and the CPA WebTrust. WebTrust will be discussed in more detail in the section that compares government and industry best practices (see pp. 24-26). Other seals, such as the PricewaterhouseCoopers Betterweb seal, are not discussed because they are broader seal programs. For example, privacy is only one part of the Betterweb seal program, which extends to sales terms, service, and customer complaints.

TRUSTe

TRUSTe was formed in order to provide a type of "Good Housekeeping Seal of Approval" for consumers to easily recognize when visiting websites. Beginning in 1996 with a small group and expanding rapidly, TRUSTe has sponsored members from major companies on the Internet. The number of websites who license the TRUSTe seal is growing. In order to post a TRUSTe seal, businesses must have a privacy policy, give notice of the use of personally identifiable information, let consumers choose how the information is used (opt-out at a minimum), and provide for security and accuracy of information. In addition, TRUSTe runs an oversight and resolution function that investigates and handles complaints. Minimal requirements for approval of the privacy statement (TRUSTe, 2000) include information about:

- The type of information collected
- Who collects it and how it is used
- Whether information is shared
- A minimum of an opt-out provision for consumer choice
- Security measures
- How to correct information

The BBBOnline Program

To participate in the BBBOnline Privacy Program, and to post the BBBOnline Privacy Seal, the company must be in good standing overall with the Better Business Bureau and have appointed a particular individual for overseeing the privacy program. BBBOnline also has a complaint resolution division and investigative function. Site policies are reviewed both initially and annually. An easily accessible and readable privacy policy must be posted that describes the following elements (BBBonline, 2000):

- the type of personally identifiable information collected
- how the information will be used and shared (only with an opt-in permission from individuals when it is sensitive information)
- access and correction procedures
- whether hidden data collection is used (such as cookies) and whether it is linked to personally identifiable information
- security information and policies
- whether information is aggregated and used for marketing purposes
- whether opt-in or opt-out is offered for the use of information in marketing

Recently, a new industry group, known by the name eGovernment Web Privacy Coalition, has emerged to try to lead self-imposed privacy standards for e-government. In its infancy, this coalition is an interesting combination of representatives from private industry, the federal government, as well as state and local governments (http://www.napawash.org/privacy). Explanations can be gleaned from the interests of the private sector in providing outsourcing for government services.

Lastly, the Network Advertising Initiative (NAI) responded to the FTC call for regulation with a proposed framework for its members (90 percent of the industry are NAI members). The framework would operationalize the four principles of notice, choice, security, and access. The NAI proposal would require members to work with a privacy-seal type organization to ensure enforceability as well.

Summary of Issues

The overall state of affairs with respect to privacy and data collection in the business world is that privacy concerns of individual consumers still exist. In particular, consumers are worried because technology allows huge amounts of data to be collected easily by businesses, with or without their knowledge — data that can then be aggregated and cross-referenced with other sources of data. While legal restrictions do exist, they are usually tied to particular events. Self-regulation by industry leaders is the most visible response of businesses to consumers' privacy concerns.

Electronic Government

Definitions and Background

Electronic government has been defined as "the continuous optimization of service delivery, constituency participation, and governance by transforming internal and external relationships through technology, the Internet, and new media" (Gartner Group, May 2000). Thus, e-government can be considered through two lenses: the type of relationship and the stage of integration.

Types of E-government

E-government can involve electronic relationships between the government and different levels of constituents. Building on the categories suggested previously by other writers, we offer a more complete view of the multidimensional relationships between governments and the entities with which they interact.

- *Government Delivering Services to Individuals (G2IS):* In this case the government establishes or maintains a direct relationship with citizens in order to deliver a service or benefit. This would include the Social Security Administration in its delivery of benefits, for example. It can also involve two-way communications as, for example, when individuals request information about benefits or the government needs information to process benefits.
- *Government to Individuals as Part of the Political Process (G2IP)*: This is the relationship between the government and its citizens as part of the democratic process. It is perhaps the most essential relationship between a government and any entity. Examples include voting online and participating in requests for comments online during the regulatory process.
- *Government to Business as a Citizen (G2BC):* Although businesses do not vote, and thus the relationship between businesses and the government will not look exactly like the G2IP, there are still opportunities for businesses to relate to the government in a citizen-like capacity. Providing Securities and Exchange Commission filings online and paying taxes online would be examples of the relationship between government and businesses in this category.
- *Government to Business in the Marketplace (G2BMKT):* While businesses can receive many online services from government, a major portion of online transactions between the government and businesses involve procurement — the hiring of contractors or the acquisition of goods and services by the government. There is substantial benefit to be gained in G2BMKT in terms of procurement for the government. Efficiencies can be achieved by reducing paperwork, mailings, and time delays, to name a few. Agencies could also group together (like consumer buying groups) to negotiate better prices. E-procurement "is one of the fastest growing areas of e-business because it can save time and money" (Symonds, 2000). These same applications could be used in other types of e-government, leading to substantial savings. For example, the purchasing department of Australia's Department of Natural Resources and Environment reported 70 percent more effi-

ciency after deploying a paperless system (Symonds, 2000).

- *Government to Employees (G2E):* Online relationships between government agencies and their employees face the same requirements as the relationships between businesses and their employees. For example, government agencies can use an intranet to provide information to their employees and can typically allow some online transactions with their employees if they have the proper technological architectures. This relationship should be distinguished from the same individual's relationship under G2IP and G2IS.

- *Government to Government (G2G):* Government agencies must often collaborate and/or provide services to one another. There are substantial gains from conducting some of these transactions online. Government-to-government applications can be performed between federal agencies, or between federal, state and local agencies. An example of an inter-governmental level e-government application is the National Science Foundation's request that all proposals for research funding by public academic institutions be submitted by an online application called FastLane (http://www.nsf.gov). The potential for G2G to benefit the government agencies involved is tremendous. There are currently over 20,000 websites for the federal government (Thibodeau, 2000). By linking sites together the agencies can reach economies of scale, and FirstGov.gov is the first attempt to do just this.

Stages of Electronic Government

The government can use different levels of technology and different levels of sophistication while developing the potential of e-government. Commentators have identified four stages of electronic government, and we add a fifth to more completely represent the set. The stages are discussed beginning with the least and moving to the most advanced.

1. *Information.* Information dissemination is the most basic form of e-government, where the government simply posts information on websites for constituents. Thousands of such sites exist. The biggest challenge with them, however, is to ensure that the information is available, accurate, and timely (Gartner Group, January 2000). Two examples are the informational web pages of the White House (http://www.whitehouse.gov/) and the U.S. Department of Transportation (http://www.dot.gov/).

2. *Two-way Communication.* In this stage, government sites allow constituents to communicate with the government and make simple requests and changes. Several of these sites are based on e-mail exchanges, and there are thousands of this type as well. Agencies allowing online requests provide sites where individuals can fill in information requests. The information is not returned immediately online but sent by regular mail in paper form or returned by e-mail. Good examples of this type of site are the Social Security Administration's websites where constituents can apply for new Medicare cards or request benefit statements (http://www.ssa.gov/).

3. *Transaction.* At this stage, the government has sites available for actual transactions with constituents. Individuals interact with the government and conduct transactions completely online, with web-based self-services replacing public servants in these cases. Actual online transacting is the most sophisticated level of e-government currently widely available. There are several hundreds of these sites. Examples include renewing licenses, paying fines, and applying for financial aid. Another example is the Internal Revenue Service's online tax-filing capabilities for individuals (http://www.irs.ustreas.gov/elec_svs/efile-ind.html). Such sites offer many benefits. For example, Arizona's system to renew vehicle registration online has dramatically reduced waiting lines at Division of Motor Vehicles offices (Thibodeau, 2000).

4. *Integration.* In the integration stage, all government services are integrated. This can be accomplished with a single portal that constituents can use to access the services they need no matter which agencies or departments offer them. One of the biggest obstacles to more online transactions between the government and its constituents is the lack of integration of all online and back-office systems. Government agencies spend expensive and time-consuming resources to have face-to-face interactions with individuals. For example, in the Kentucky governor's

office, up to 90 percent of customer interactions are face-to-face (Thibodeau, 2000). Integrating online systems and back-end systems to support these customer requests could save time and money for the agencies involved, as well as improve customer service. Two portals for e-government integration include Australia's state of Victoria (maxi) and Singapore's eCitizen Centre. Recently, the U.S. government also established a portal and is committed to working towards a site that is integrated and organized according to the user (http://firstgov.gov/).

5. *Participation.* These are government sites that provide voting online, registration online, or posting comments online. Although this could be seen as a subset of the two-way communication stage, we see this as so significant as to warrant a separate category. In particular, when viewing the effect of privacy concerns on the provision of electronic government, it is helpful to view this function as distinct because of the unique sensitivity of providing this online feature. There are few government sites that provide for this level of electronic sophistication. One of the most prominent future uses of online transaction-based e-government with the federal government may be for individuals to vote over the Internet. The California Internet Voting Task Force (http://www.electioncenter.org/voting/voting_report.htm) reported findings in January 2000 and recommended a phased-in approach, with great care for authentication and security. Online voting will require technologies to support the privacy of individual voters while allowing recounts and authentification of identity (Gartner Group, January 2000).

Electronic Government Framework

The model illustrated in Table 1 represents the convergence of e-government stages and categories of relationships between the government and its constituents. It is important to establish this framework in order to determine the areas in which privacy is crucial in the process.

Table 1: Electronic Government Framework with Examples

	STAGES OF E-GOVERNMENT				
	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5
Type of government	Information	Two-way communication	Transaction	Integration	Political participation
Government to Individual — Services	Description of medical benefits	Request and receive individual benefit information	Pay taxes online	All services and entitlements	N/A
Government to Individual — Political	Dates of elections	Receive election forms	Receive election funds and disbursements	Register and vote. Federal, state and local (file)	Voting online
Government to Business — Citizen	Regulations online	SEC filings	Pay taxes online Receive program funds (SBA, etc.) Agricultural allotments	All regulatory information on one site	Filing comments online
Government to Business — Marketplace	Posting Request for Proposals (RFP's)	Request clarifications or specs	Online vouchers and payments	Marketplace for vendors	N/A
Government to Employees	Pay dates, holiday information	Requests for employment benefit statements	Electronic paychecks	One-stop job, grade, vacation time, retirement information, etc.	N/A
Government to Government	Agency filing requirements	Requests from local governments	Electronic funds transfers		N/A

Electronic Government, Data Collection, and Privacy

Integration of Government Services and Privacy

The intersection of privacy interests and the implementation of information technology (IT) and electronic government to enhance efficiency and ease of use for citizens is not a simple topic, but a dynamic and multifaceted one. Paradoxically, but understandably, laws and executive orders both mandate action and restrict the government in its pursuit of these goals.

A brief history of the federal government's commitment to delivering services via the Internet while maintaining the privacy and security of information is important background. In 1993, President Clinton established the Information Infrastructure Task Force (IITF) and charged it with leading and developing the National Information Infrastructure (NII). As part of its work, the task force's Privacy Working Group compiled the report "Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information" (Principles; June 6, 1995; available at http://www.iitf.nist.gov/ipc/ipc/ipc-pubs/niiprivprin_final.html). While recognizing the immense potential for the use of the NII, the introduction states:

> These benefits, however, do not come without a cost: the loss of privacy. Privacy in this context means 'information privacy,' an individual's claim to control the terms under which personal information — information identifiable to an individual — is acquired, disclosed, and used.

Recommended to apply to both public and private uses of private information, the principles (Figure 1) set forth more detailed standards under the three fundamental areas of "information privacy, information integrity, and information quality." A follow-up document was also produced by the task force: "Options for Promoting Privacy on the National Information Infrastructure," (April 1997; available at http://www.iitf.nist.gov/ipc/privacy.htm). Although having no rule of law, the principles act as a statement of privacy principles for future policy development.

Vice President Gore also led a task force to address issues associated with the infrastructure and systems of government, called the National Performance Review. An outgrowth of this review was the creation of a working group known as the Government Information Technology Services (GITS) — now subsumed within the Chief Information Officers Council — and its subsequent work to implement the infrastructure recommendations aimed at establishing e-government capabilities and efficiencies. In 1996, the report "Access America" (available at http://www.accessamerica.gov/reports/public2.html) summarized the administration's approach, steps toward achieving the goals, and action items. Several sections of the report relevant to this study of privacy and the delivery of government services electronically provide background for the more

Figure 1: Principles (Information Infrastructure Task Force; Privacy Working Group)

Information Privacy
1. Respect individual privacy
2. No improper alteration or destruction
3. Accurate, timely, complete, and relevant

Principles for Providers of Information
1. Awareness: personal responsibility to obtain information about collection and use
2. Empowerment: should have a way to access, correct, technically control information and to be anonymous in certain cases
3. Redress: when harm occurs

Principles for Users of Information
1. Impact assessment
2. Only reasonably necessary
3. Notice; why, what, protections, consequences and redress
4. Security
5. Only according to individual's understanding of use (unless "compelling public reason")
6. Education for users and public

recent legislative and administrative actions relevant to e-government and privacy. The relevant sections include:

- *A01: Improve the Public's Access to Government Services. Section 2.* Incorporate technology that will assure the public of security and privacy in their transactions. The teams developing public access systems should identify their security and privacy requirements to the GITS Board Security and Privacy Champions. The GITS Board should promote the development, testing, and use of methods that will assure the public of the security and privacy of their electronic transactions.
- *A14: Guarantee Privacy and Security.* Recommends to 1) create a privacy "champion" within the GITS Board, 2) complete the privacy work of the IITF, and 3) accelerate work on digital signatures and encryption.
- *A15: Integrate the Government Services Information Infrastructure.*

On December 17, 1999, President Clinton issued a memorandum on Electronic Government (http://www.cio.gov/docs/ElectronicGovernment Memo.htm). The memo directed agencies to put forms for the top 500 government services online by December 2000, and ordered all federal agencies to continue to develop and post privacy policies on their websites. The memo emphasized that services should be delivered through "private and secure electronic use of the Internet." On June 2, 1999, the director of the Office of Management and Budget (OMB) issued guidelines for agencies in designing the privacy portions of their websites (http://www.cio.gov/docs/webprivl.htm). These guidelines encourage privacy disclosures to be in plain and understandable language, to describe information automatically collected (such as cookies) through e-mails, electronic forms, and information collected for security purposes. In addition, if the Privacy Act (discussed below) is implicated by creating a system of records, then a link to information about the act should be provided. On June 22, 2000, a memo from OMB further directed federal agencies to limit the use of cookies on their sites (http://www.cio.gov/docs/lewfinal062200.htm). The memo states, "Because of the unique laws and traditions about government access to citizens' personal information, the presumption should be that 'cookies' will not be used at federal websites." Only when there is a compelling reason, approval from the agency head, and the website uses clear and conspicuous language to give notice of the practice may an agency use cookies.

Overview of Data Collection Practices in E-Government

Government agencies have access to the same technologies that businesses do with respect to collecting, aggregating, and cross-referencing individuals' data. Unlike businesses, though, agencies must report their data collection practices to OMB. Two of the main statutes with respect to data collecting by the federal government — the A-130 Biennial Privacy Act report and the Computer Matching Act — will be presented in the Limitations on Government Data Collection section (see pp. 21-22).

As with businesses, the main issues regarding data collection of private information center around the issues of faster and easier collection of data, data being collected without the individual's knowledge, and cross-referencing data from multiple sources. The discussion of the limitations on government data collection will highlight the requirements for agencies to notify individuals when data is collected and how it will be used. Cross-referencing of data contained in computer records of federal agencies is not new, but it is the amount of data collected that is now the issue. Table 2 presents a summary of computer data matches that were allowed between agencies based on the 1994/1995 Computer Matching Tables of OMB.

Agencies share information with other agencies for various purposes. Some of the matches allowed as reported in the table have expired since 1995, but the table shows that federal agencies mostly match personal data for debt collection purposes (as allowed by the Computer Matching and Privacy Protection Act described later). An example of debt collection would be the Department of Education matching data with the Postal Service to identify postal employees delinquent on student loans to initiate debt collection. An example of eligibility verification would be the Department of Education matching data with the Social Security Administration to verify the Social Security numbers and citizenship of student aid applicants. The Department of Education matching data with the Internal Revenue Service to locate taxpayers who have defaulted on student loans is an example of agencies sharing data for the purpose of fraud and/or ineligibility detection. Finally, data reconciliation involves two agencies sharing information to update records. For example, the Department of Labor may match data with the Office of Personnel Management in order to determine the correct amount of retirement benefits based on workers' compensation income.

It should also be noted that in the absence of government provision of online services, the private sector has become involved as an intermediary in providing these services to citizens. The National Information Consortium (NIC), ezGov.com, and GovWorks.com are all involved in some way with bridging the gap between government and citizen transactions. Paying traffic tickets online and retrieving electronic public information online (for a fee) are examples of such transactions (Manjoo, 2000).

Consumer Privacy Concerns in E-Government

Unlike the private sector, there have been no repeated studies of constituent perceptions of the privacy and security of Internet transactions at federal websites. This is an area that should be studied, taking into consideration the relationships and stages of e-government presented earlier. There is anecdotal evidence that public perceptions will affect the implementation of electronic government, adding an additional layer to the legal limitations. Below is a sampling of public issues regarding privacy of information and e-government.

- One of the most sensitive areas of personal information is the Social Security number (SSN). Access to an individual's SSN can facilitate the collection of additional information and can lead to identity theft. The Social Security Administration (SSA) recently agreed not to send checks through the mail that reveal a person's SSN through the envelope. In 1996, when the SSA allowed individuals to access their personal benefit statement on the Internet, an outcry arose about the lack of sufficient security on the system. Access was subsequently modified to require an additional e-mail request as compared to the original, more immediate access. Lastly, there is a statute pending in Congress that proposes further protection of SSN's, although critics say that the exceptions thwart the privacy of individuals.

Table 2: Summary of Computer Matching Data for 1994/1995

		Purposes			
Agency	# of agencies matching data with	Eligibility verification	Debt collection	Fraud/ineligibility detection	Data reconciliation
Dept. of Agriculture	2		2		
Dept. of Defense	34	5	22	6	1
Dept. of Education	8	2	2	4	
Dept. of Health and Human Services	33	13	4	10	6
Dept. of Housing & Urban Development	5	1	3	1	
Dept. of Justice	5	4		1	
Dept. of Labor	6	1	1	2	2
Dept. of Treasury	9	2	4	3	
Dept. of Veterans Affairs	18	6	5	5	2
Office of Personnel Management	15		3	7	5
Selective Service System	1			1	
Railroad Retirement Board	13		3	4	6
U.S. Postal Service	18	1	13	3	1
Environmental Protection Agency	1			1	
National Science Foundation	2		2		
Small Business Administration	3	1	2		
Total	173	36	66	48	23
Percent		21%	38%	28%	13%

- There is a currently a debate about the public information found in bankruptcy filings, with some fearing that the detailed financial information found in the filings could lead to fraudulent activity.
- Virginia's State Bar section on family law is organizing to lobby against the posting of divorce information online. The personal and property information listed, they believe, could present unwarranted negotiating positions and a possibility for identity theft.
- A recent survey showed that 65 percent of people support deliberative electronic government development. When asked to rate the reasons for implementing e-government, greater accountability to the citizens outranked better delivery of government services by almost three to one (NUA Internet Surveys, 2000).

A recent modest survey undertaken after the security breach at Los Alamos found that consumers were more likely to trust business to secure their private information and had concerns about the misuse of information in government's hands (ITAA, 2000). A survey of federal and state websites also showed that privacy and security statements are lacking on these sites (West, 2000).

Limitations on Government Data Collection

Traditional limitations on the power of government to intrude into citizens' lives begins with the United States Constitution. The police power of the government and law enforcement is limited. In addition, the ability of government to pass regulations in private areas is limited by the penumbra of rights protecting a citizen's right of privacy. Because this report focuses on the collection of data, however, we do not discuss the well-known Constitutional limitations on search and seizure and the limitations of regulation in areas such as reproduction and other personal privacy rights. It is important to note the existence of these protections as part of the underlying and fundamental policy of constraining government actions and protecting citizen privacy.

Data collection by the federal government is regulated by two primary statutes and various other laws applying to specific agencies (for example, the Internal Revenue Service and the Census Bureau). Because the Privacy Act and the Computer Matching Act are the main statutes affecting all agencies, these will be the focus of this discussion. The Freedom of Information Act (FOIA) allows access to government information under the goal of openness and accountability. This act is counter to the Privacy Act, but exceptions to the release of certain information make the FOIA relevant to a study of privacy in e-government as well. Concerns about the government's ability to amass information using new technologies emerging from the computer age are not new. In 1974, when the Privacy Act (5 U.S.C. § 552a) was passed, there were concerns surrounding the surveillance activities unveiled during the Watergate investigation. The Privacy Act takes an overall view regarding the collection and use of personally identifiable information by federal agencies. Any agency that maintains a system of records that collects information about an individual that is identifiable by name, number, or other identifier must:

1. Give notice in the Federal Register when new systems of records are created.
2. Make systems of records accessible.
3. Inform the individual when information is being collected and about its purpose, and disclose the possible consequences of nonparticipation.
4. Obtain permission from the individual to share the information.
5. Give individuals the right to review records and disclosures of records and to submit corrections.
6. Ensure the accuracy (obtain information directly from the individual when possible) and security of information.

There are, however, 12 exceptions to the limitation on disclosure without the person's consent. Most applicable to our study of individual privacy and e-government are two: intra-agency use on a need-to-know basis, and routine uses that are consonant with the reasons the information was collected. The broad interpretations given these exceptions, resulting in widespread sharing without consent, have been criticized (Bevier, 1995).

Congress amended the Privacy Act in 1988 with the Computer Matching and Privacy Protection Act. Applicable to debt collection or benefit decisions made through computer matching, the act requires notice to the individual and an opportunity to correct information. Additionally, agencies must have Data Integrity Boards perform cost-benefit analyses and report their matching activities.

On May 14, 1998, President Clinton issued a directive for agencies to review their systems of records in light of the Internet and electronic methods of communication and to appoint a senior agency member to be responsible for privacy (http://www.whitehouse.gov/OMB/memoranda/m99-05-a.html). The memorandum stated, "As development and implementation of new information technologies create new possibilities of the management of personal information, it is appropriate to reexamine the federal government's role in promoting the interest of a democratic society in personal privacy and the free flow of information."

The OMB guidelines (http://www.whitehouse.gov/OMB/memoranda/m99-05-b.html) for complying with the memorandum outline and restate the requirements of the Privacy Act, and emphasize the necessity for review of agency records and security features in the electronic environment. In making changes to out-of-date records, and adding new record keeping because of the Internet, accuracy and completeness were emphasized. In addition — and particularly relevant to the pursuit of electronic government — are the guidelines noting that systems should not be "inappropriately combined," and that pursuant to the initiative to share records with state and local governments, agencies should consider the purposes and security of information sharing under the routine-use exception of the Privacy Act. One interpretation of the presidential memo and the guidelines is that the goal of electronic and integrated government services, both federal and state, is paramount to the limitations on sharing information under the Privacy Act.

The Freedom of Information Act is based on the premise that open government records provide transparency and accountability. FOIA requires the disclosure of public records, with the exception of personal data that would amount to an "unwarranted invasion of personal privacy." Included are personnel and medical files. FOIA also includes an exception that is important for businesses, allowing for the privacy of information about trade secrets. Individual states also have FOIA acts.

Government Paperwork Elimination Act (GPEA). GPEA, which was passed in 1998, requires governmental agencies to provide the ability for those dealing with them to complete electronic transactions and use electronic signatures by October 21, 2003. (While there is some overlap with the E-SIGN legislation, governmental agencies are primarily covered by the GPEA). The following is a summary of the act and its implementation by agencies:

> GPEA recognizes that building and deploying electronic systems to complement and replace paper-based systems should be consistent with the need to ensure that investments in information technology are economically prudent to accomplish the agency's mission, protect privacy, and ensure the security of the data. Moreover, a decision to reject the option of electronic filing or record keeping should demonstrate, in the context of a particular application and upon considering relative cost, risks, and benefits given the level of sensitivity of the process, that there is no reasonably cost-effective combination of technologies and management controls that can be used to operate the transaction and sufficiently minimize the risk of significant harm.

Driver's Privacy Protection Act (18 U.S.C. § 2721) (DPPA). The 1994 DPPA was recently upheld by the United States Supreme Court in *Condon v. Reno*. The court affirmed the federal right to limit the driver's license information sharing of states to commercial entities. South Carolina had been selling such information for $600,000 per year.

Various State Statutes. It is beyond the scope of this report to list all of the state limitations on public record sharing, but a few examples illustrate the nature of state and local approaches.

- A recent Colorado case upheld the right of the judiciary to restrict access to records to those who are physically present at the court site. In essence, this will preclude any remote public access electronically.
- A Cookeville, Tennessee, ordinance specifically exempts public records from being shared in an electronic format requirement.
- A California law prohibits the release of arrestees' home addresses for commercial reasons. This law was recently upheld as constitutional by the United States Supreme Court in *LAPD v. United Reporting Publishing,* 1999.
- Oregon law limits access to driver's license information.

Best Practices in Private and Public Privacy Standards

We now turn to a comparison of the best practices in privacy standards of businesses and the government by looking at their self-regulation attempts. In this comparison, CPA/WebTrust privacy seal program requirements are used to represent a best practice in self-regulation by businesses. The WebTrust Privacy Principle states:

> The entity discloses its privacy practices, complies with such privacy practices, and maintains effective controls to provide reasonable assurance that personally identifiable information obtained as a result of electronic commerce is protected in conformity with its disclosed privacy practices. (3.0)

This principle is further organized into four areas: disclosures, policy, technology, and procedure and enforcement (monitoring and performance).

We can compare the criteria for WebTrust with the federal government disclosure practices as outlined in the June 2, 1999, *Guidance and Model Language for Federal Web Site Privacy Policies* and the June 22, 2000, *Memorandum on Privacy Policies and Data Collection of Federal Web Sites*. These two memoranda address the use of cookies by federal websites and their privacy policies. In the June 2, 1999, document, five areas are discussed:

1. Introductory language
2. Information collected and stored automatically
3. Information collected from e-mails and web forms
4. Security, intrusion, and detection language
5. Significant actions where information enters a system of records

We can also use the Internal Revenue Service "Privacy Impact Assessment" that was identified as a federal government best practice by the February 25, 2000, memo from the CIO Council Subcommittee on Privacy. We can also assume that Privacy Act requirements will be followed. Table 3 presents these comparisons, using the CPA WebTrust seal program as the baseline. The comparisons are not exact, but credit is given when areas are substantially similar. However, two particular facts deserve note. The IRS best practice applies only to new systems. It does not apply, in general, to existing ones, thus severely limiting its effect. The Privacy Act applies only to systems of records. It is surprising that the fifth element of the June 2, 1999, memo states, "To date, a large fraction of federal web pages have not collected significant amounts of identifiable information in ways that entered directly into systems of records covered by the Privacy Act." Thus, Table 3 may overstate the effect of the Privacy Act on federal websites.

Table 3: Comparisons of Best Practices in Industry and Government

CPA WebTrust Privacy Principle	Federal Disclosure Policy	IRS Best Practice	Privacy Act
DISCLOSURES			
What information is collected*	✓		✓
Where the information is obtained			✓
How it is maintained			
How it is used*	✓		✓
Whether it is shared with third parties	✓		
An opt-out choice for personally identifiable data collection			
Opt-in for providing sensitive information (such as medical information)			✓
Consequences of opting out			✓
Process for review and correction of information			✓
How hidden tracking is used and consequences of disabling them (such as cookies)	✓		
Dispute resolution process			✓
Changes or updates of information			✓
POLICIES			
Policies and objectives "consider"; • notice, choice, access, security, and enforcement		✓	
Employees follow policy			
Person in charge of policy			
Adequate security (backup, storage, and restoration)		✓	
Policy consistent with disclosures			
SECURITY			
Procedures for new users		✓	
Procedures for authentication of authorized users		✓	
Users can change, delete, or update their information			
Limitation of remote access to those authorized			
Controlled access; only to own personal information			
Encryption provided			
System protected from outside access			
PRIVACY SPECIFIC			
E-commerce private information • Sharing limited to essential parties • Customer notified when data collected, or permission obtained after, for release to third parties • Employees use this information only for business purpose			✓
Personally identifiable information is accurate and complete for intended purpose			✓
Procedure for assessing that third parties with whom information is shared have adequate privacy and security	✓		
Permission is obtained to store information on the customer's computer (such as cookies), or customer told how to prevent such	✓		
Less restrictive change in policy does not affect previously collected identifiable information unless customer is given clear and conspicuous choice			
MONITORING/PERFORMANCE MEASURES			
Procedures for monitoring security			✓
Procedure for keeping disclosures current and consistent, including regulatory compliance			✓
Security and systems are tested and updated			✓
Breaches are monitored and fixed			✓

** The IRS Best Practices does refer to and incorporate the Privacy Act.*

In summary, the comparisons are not exact, but do serve to show that industry best practices have gone far to identify complete privacy practices for the collection of information, perhaps more so than the federal government. The limitation of the IRS best practices to new systems only is one example. Federal policies and standards are often found in general language. Under the WebTrust seal program, the business must undergo audits at regular intervals to keep the seal. The specific requirements that are monitored by an outside third party lend credibility to the evaluation and seal. The comparison also shows that federal practices are found in multiple places and could benefit from a summarized and central document applying to all agencies, similar to the way that WebTrust can be applied to many different industry members.

The comparisons do not, of course, show whether industry is following these best practices, as most electronic businesses are not members of a WebTrust type program. However, the comparisons are instructive as e-government seeks to make the online experience for citizens a trustworthy experience. If, for example, the disclosures that are made on government sites are less detailed and harder to find than those on commercial sites (as the comparison would seem to indicate), then citizens may find the government sites less trustworthy. Another element of trust involves the collection of information surreptitiously. Although government agencies were directed not to use cookies without prior approval and clear and conspicuous notice, a study recently revealed 13 federal government sites that violate that policy. The U.S. Forest Service International Programs website also used a third party to collect and compile information about the users of the website (*Richmond Times Dispatch*, 2000).

Case: FirstGov.gov

FirstGov.gov is the first true portal service created for the U.S. federal government (http://firstgov.gov/). The site does not provide complete access to all services, but the U.S. government has stated it will continue to work toward a site that is integrated and organized according to the user. The site advertises itself as "Your First Click to the U.S. Government." As such, it provides integration services (stage four of the e-government framework) with access to topics (instead of agencies) as well as featured subjects, information about the three branches of government, and other links of interest. Its privacy link is highly visible on its navigation bar at the top of the page and right next to the main page link. The privacy policy is very clear: *"We will collect no personal information about you when you visit our website unless you choose to provide that information."* While the statement is easily understandable by all constituents, further explanations under the section "Information Collected and Stored Automatically" include details of what is collected automatically when individuals just browse through the web pages or download information. It states: *"This information does not identify you personally."* Yet the list of information automatically collected includes:

1. The Internet domain (such as vt.edu) and the IP address of the computer used to browse the page
2. The type of browser and operating system used
3. The data and time of the access to the site
4. The page visited
5. The address of the referring page

This information is collected *"to help us make the site more useful to visitors — to learn about the number of visitors to our site and the types of technology our visitors use. We do not track or record information about individuals and their visits."* However, when obtaining IP address information and domain information, the government could easily track a large number of individuals who access the site from their own computer, either as their office computer or home computer (depending on connection type). As such, the IP address, coupled with domain information, is identifiable. FirstGov.gov should therefore be careful in saying that the information cannot identify individuals. They may make no attempt to trace back the individual Web surfers to their site, but they have the means with the information collected to do so. Language used in this privacy policy may need revisions.

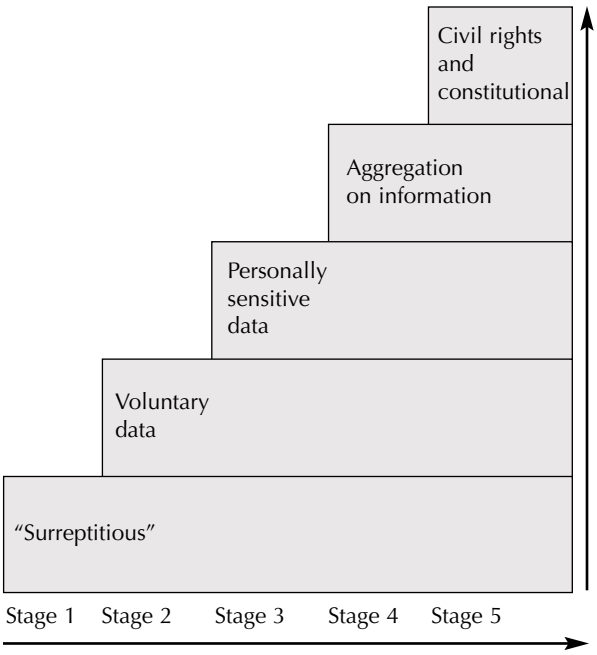
Recommendations and Lessons Learned

The findings presented in this report highlight the importance of identifying, understanding, and addressing privacy concerns in electronic government. The report proposes an e-government framework that identifies six constituent relationships and five stages of e-government. The combination of relationships and stages of e-government are more complex than in electronic commerce in general. As such, these relationships need to be taken into account when the government is considering the level of privacy and concerns about privacy and security by its constituents. For example, in the integration stage, where government services are all accessible through one portal, the government should ensure that all privacy and security practices are consistently displayed no matter what direction an individual is taken on the site when requesting information. It is also important to realize that as government agencies move through the stages of e-government, the level of data collection and constituent privacy concerns increase.

Figure 3 graphically depicts the increases in data collection and related privacy concerns through the stages of e-government. It clearly indicates that these increases are cumulative. For example, as the government becomes more interactive and moves toward electronic participation of citizens in the political process, levels of privacy concerns are heightened. It should also be noted that there is an increased level of privacy concerns when third parties are involved. This would typically occur starting at stage 3. A more detailed description of data collection practices at each stage is presented below:

- Stage 1: Information. Only "surreptitious" data collection is performed, possibly through cookies, since there is only one-way communication.
- Stage 2: Two-way Communication. Participants can enter data themselves for participating in an information exchange, and therefore there is an increased amount of data available.
- Stage 3: Transaction. Since transactions require more sensitive information to be shared, such as credit cards, data collection and possible privacy concerns increase.
- Stage 4: Integration. At this stage, sources of information are integrated. While this provides numerous advantages, it also increases the probability that information can be shared between various agencies.
- Stage 5: Political Participation. Stage 5 represents one of the most sensitive uses of information because there are constitutional and civil rights implications to use of this data. The most stringent security and privacy practices are required to create trust and protect the fundamental rights of individuals at this stage.

Figure 2: Level of Data Collection and Privacy Concerns for E-Government Stages



Recommendations

The issue of privacy for electronic government is a complex one that requires a thorough investigation of the implications for all constituents. There are some recommendations that can be made based on the findings presented in the report. This section presents these recommendations organized into four broad categories. Specific recommendations are then provided within each.

Recommendation 1. The government must meet the legal requirements to instill confidence and trust in government.

There are three main legal constraints on the federal government's ability to collect and share information: the Privacy Act, the Computer Matching Act (part of the Privacy Act), and the Freedom of Information Act. The government cannot assume that the laws protecting privacy will address public perceptions and business concerns without a systematic and understandable method of communicating the application of the laws to the particular transaction. In addition, the position taken by this study is that the government must go beyond the mandates of the law, staying within the FOIA, in order to address the concerns and distrust of the public in using electronic government.

Recommendation 1A. Make electronically available, in an easy to read and understandable format, the intent to exempt records from disclosure under FOIA.

Both individuals and companies may be fearful of privacy invasions when an agency keeps records of sensitive information. To encourage the use of electronic government and to allay these fears, bold and clear information is necessary. Too often, the "fine print" of agency intent is hidden in the mandatory Federal Register publication. For example, the FTC created a system of records to collect information under the Identity Theft and Deterrence Act. The admirable goal of centralized collection can help alert others to methods of fraud and help law enforcement track perpetrators. *However*, a person may understandably be reluctant to fill in the online form sharing financial information and details of the fraud when visiting the FTC website and seeing the statement that information may be released when requested under FOIA. It is only when accessing the long and complicated Federal Register document that one can find the statement that the FTC intends to treat this information as personal and confidential, excepting it from disclosure under FOIA. A system that is standardized throughout federal agencies would help individuals and businesses easily determine, when appropriate, whether information will be disclosed.

Recommendation 1B. Review the business confidential and trade secret information exception to FOIA for timeliness in the electronic environment.

This recommendation applies to the exception to the public availability of business trade secrets and sensitive information. If electronic government is to succeed, then businesses must be reasonably assured that the confidential information that they supply to government will not be released. When the G2BMKT progresses to stage 3, and especially to stage 4, the possibility for electronic information release increases. Businesses must be convinced that the risk and cost of disclosure is small compared to the benefits of participating in the market. Technical as well as legal methods of protecting business information should be sought in order to protect information in a consistent way, especially when it is accessible across agencies. FOIA should be studied to determine whether more specific protections for business are warranted.

Recommendation 1C. Make disclosures under the Privacy Act available electronically, in standard and easily readable form.

The Privacy Act requires disclosure of the system of records and other information in the Federal Register. However, once again, the Federal Register is a difficult document for most consumers and users to navigate. The Privacy Act grants individuals most of the protections identified by consumers as important in their use of e-commerce — disclosures, opt-in, access, accuracy, and security. A "consumer friendly" version of the disclosures could supplement the mandatory disclosures and would help users of e-government with readily accessible information about privacy that may encourage them to share information.

Recommendation 1D. Consider the collection of IP addresses as "personally identifiable information" under the Privacy Act.

The Privacy Act applies only if the information about an individual is personally identifiable. As explained in a review of the FirstGov website, IP addresses may be used to identify the individual later. Although it is unclear whether the collection of IP falls under the letter of the Privacy Act, government should err on the side of creating trust. Government should learn from the DoubleClick experience and either not collect IP addresses or pledge not to use this information in personally identifiable ways.

Recommendation 1E. Review the efficiency of Data Protection Boards under the Computer Matching Act.

Data Protection Boards may provide useful information about whether the decentralized nature of the review of necessary computer matching is workable in the case of large numbers of varied electronic records. In the e-commerce world, businesses have not only begun to appoint individuals in charge of privacy, but many have joined to standardize and adopt methods of privacy in cross industry groups. These are discussed more fully in the recommendation relating to privacy seals. However, a study of the presently constituted Data Protection Boards could encourage the development of a similar government-wide data protection board. The legal avenue for resolving privacy disputes is cumbersome and costly. To the extent possible, dispute resolution must be addressed through an ombudsman or data protection board.

Recommendation 2. The government must gain individual confidence and trust by addressing privacy perceptions.

Recommendation 2A. Conduct repeated, longitudinal e-government privacy studies.

The research conducted for this report reveals that in contrast to the private sector, there have been no longitudinal studies of constituent perceptions of privacy with respect to the federal government. We recommend that a series of privacy studies be conducted that would investigate the trust, fears, concerns, and opinions of constituents toward privacy of transactions with the federal government. In addition, a study of federal websites should be undertaken as well. Conducting a series of repeated studies will allow the government to evaluate the trends in constituents' perceptions, indicating changes in opinion about how the federal government handles privacy concerns with respect to e-government, and will benchmark the progress of federal websites in addressing these concerns.

Studies should recognize the different relationships inherent in e-government. Consumers are sensitive to the collection and use of information. This extends to information that is now publicly available, which takes on a new meaning when posted electronically. It also applies to the use of information for commercial purposes, and the outsourcing of information technology. It should be noted that this recommendation applies to all types of e-government where individuals are involved (G2I-Services and G2I-Political), as well as businesses. In addition, when the government deals with its own employees, there are heightened privacy protection requirements by law.

Recommendation 2B. Create a government privacy seal program and develop standard, precise, and clear privacy statements.

Industry best practices have gone far to identify privacy practices for the collection of information and to incorporate these practices into seal programs. The federal government should consider following this model. Once educated about the meaning of a federal privacy seal, constituents may have more confidence in dealing with federal sites that display

the seal. A federal privacy seal program can learn from the best practices of the private sector in its attempt at self-regulation.

Some elements that could be included in such a seal program, for example, include the requirement for detailed privacy disclosures. The research reported here indicates that government sites might have less detailed privacy disclosures and ones that are harder to find than those on commercial sites. The government should increase its efforts to clearly delineate both privacy and security policies on their websites by developing a set of uniform, standardized privacy notices for agencies to use. These privacy standards should be precise and clear, and refer to the actual practices used by the federal websites. They would provide uniform models depending on the type of data collection practices used at each site. This relates to the earlier recommendation addressing legal protections. The need for precise statements is underscored by the FirstGov.gov example presented in the report. While the site states that no personally identifiable information is collected, the collection of domain name and IP addresses provides the *means* to identify.

The information should also be easy to find and understand for all constituents accessing the websites. Our research has shown that privacy and security notices are found in different places on federal websites. As electronic government seeks to make the online experience for citizens a trustworthy one, the agencies should be provided with recommendations on where to place their website privacy statements. Another possibility is to have a summarized and central document applying to all agencies that do not collect private information. Sites would then point to that particular statement. The same could then be done for sites collecting sensitive information.

Once a seal program has been developed, agencies will have to follow its policies, procedures, and standards before being allowed to display the seal on their website. Since technology and information-gathering practices change rapidly in today's society, the elements of the seal program must be reviewed on a regular basis. In order for the seal program to work properly, the websites displaying the seal must also be audited on a regular basis. Assuming that such a program will provide precise and clear checklists and procedures, auditing should be more straightforward than it has been for general privacy policies. Under the present organization of the government, it is possible that the audit function could be placed under the responsibility of the Office of Management Budget. However, it would be worth considering the feasibility of using outside audits for the seal program for the increased confidence that would result from an unbiased third party opinion.

Recommendation 2C. Educate constituents on privacy and security in e-government.
The government should invest in educating its constituents about privacy and security in e-government. When uniform statements and policies are implemented, they will only be effective if constituents are knowledgeable about them. In the electronic environment, the ability to quickly recognize and understand the methods of transactions, including privacy and security, is essential for trust and usage. Just as the electronic shopping cart is now recognized and utilized, it will be important for constituents to easily and quickly understand the privacy and security level applied to their transaction.

Recommendation 3. The government must gain the confidence and trust of businesses by encouraging participation in the marketplace and creating efficiencies.

Businesses dealing with the federal government also have privacy concerns that need to be addressed. As such, recommendations 1 and 2 apply to the dealings of businesses with electronic government as well. However, there are additional recommendations that can be made for e-government to gain the confidence and trust of businesses.

Security is an important factor to consider in discussions of privacy. Security has been empirically linked to privacy and trust in prior research. Therefore, we believe the government needs to be particularly reassuring toward businesses with respect to the security of their information by using advanced technologies for security and clearly posting security statements. As businesses deal with the government, competitive, copyrighted, and confidential information will be exchanged electronically. It could be disastrous for some companies if their information went to other

businesses either because of security failures or improper access permitted to third parties. This is a particular point of importance in government dealings since subcontracting is a common practice with the federal government. As government finds it necessary to use outside IT resources, it must be vigilant in choosing partners who will be trusted with the privacy and security of citizen and other business information. Interweaving commercial with government functions should be undertaken with caution and serious study.

Recommendation 4. The federal government must work with state and local governments and agencies to develop standardization and shared privacy standards.

State and local governments are not subject to the Privacy Act, and therefore are not required to follow the fair information practices contained therein. As G2G e-government moves to stage 2 and beyond, and especially to the integration stage, it will be essential that the commitment to privacy as related to different constituents is shared.

Conclusion

The privacy and security of online transactions is an important element for facilitating e-commerce and, therefore, must be an important consideration for e-government. The use of electronically gathered information can be beneficial for planning and delivering services and efficiently allocating resources. To the extent possible, government should utilize this avenue, but always in a way that protects the privacy and security of its constituents' information.

References

Anonymous, "Protecting Your Financial Privacy: Your Finances Are Less Secure Than You Think. But The Web Can Help You Fight Back," *Money*, June 1, 2000, p. 161.

_____, "Web Site Visitors Watched," *Richmond Times Dispatch*, October 22, 2000.

Anstead, M. "Taking a Tough Line on Privacy," *Marketing*, April 13, 2000, p. 31.

Backes, Ronald, "Freedom, Information, Security," *Seton Hall Constitutional Law Journal*, Summer 2000, pp. 927-1003.

BBBonline, "Privacy Program Eligibility Requirements," http://www.bbbonline.org/privacy/threshold.asp, 2000.

Bevier, L. R., "Information About Individuals In The Hands Of Government: Some Reflections On Mechanisms For Privacy Protection," *William and Mary Bill of Rights Journal*, (4), Winter 1995, pp. 455-504.

Branscum, D. "Guarding On-line Privacy," *Newsweek*, (135:23), June 5, 2000, pp. 77-78.

Cate, Fred H. & Vann, Richard J., "The Public Record: Information Privacy and Access," 1999, available at http://www.cspra.org.

Gartner Group, "E-Government Security: Voting on the Internet," *Research Notes, Strategic Planning Assumption*, January 18, 2000.

Gartner Group, "E-Government Strategy: Cubing the Circle," *Research Notes, Strategic Planning Assumption*, April 20, 2000.

Gartner Group, "Key Issues in E-Government Strategy and Management," *Research Notes, Key Issues,* May 23, 2000.

Green, H.; Yang, C.; Judge, P.C., "A Little Privacy, Please," *Business Week*, (3569), 1998, pp. 98-99.

ITAA, "Keeping the Faith: Government Information Security in the Internet Age," available at http://www.itaa.org/infosec/faith.pdf

Johnson, Stephen, "The Internet Changes Everything: Revolutionizing Public Participation and Access to Government Information Through the Internet," *Administrative Law Review*, (50), Spring 1998, pp. 277-337.

Manjoo, F. "Pay those fines Online," *Wired News*, Aug. 24, 2000, http://www.wirednews.com/news/print/0,1294,38336,00.html

Melillo, W., "Private Lives?," *Adweek*, (40:45), 1999, pp. IQ22-IQ28.

NUA Internet Surveys, "Electronic Government Wins Public Confidence," October 2, 2000, http://www.nua.ie/surveys/.

Online Privacy Alliance (OPA), "OPA Top 100 Study," 1999.

Punch, L., "Big Brother Goes On-Line," *Credit Card Management*, (13:3), June 2000, pp. 22-32.

Sweat, J. "Privacy Paradox: Customers want control — and coupons," *Informationweek*, (781), April 10, 2000, pp. 52-53.

Symonds, M. "Government and The Internet: No Gain Without Pain," *The Economist*, (355), June 24, 2000, pp. S9-S14.

Thibodeau, P., "E-Government Spending To Soar Through 2005," *Computerworld*, (34:17), April 24, 2000, p. 12.

TRUSTe, "TRUSTe Program Principles," http://www.truste.org/webpublishers/pub_principles.html, 2000.

Wayne, Leslie, "One Consulting Firm Finds that Voter Data is a Hot Property," *New York Times*, Sept. 9, 2000, available at http://www.nytimes.com/2000/09/09/technology/09PRIV.html.

West, Darrell M., "Assessing E-Government: The Internet, Democracy, and Service Delivery," available at http://www.insidepolitics.org/egovreport00.html (September, 2000).

About the Authors

Janine S. Hiller is Professor of Business Law at the Pamplin School of Business, Virginia Tech, Blacksburg, Virginia, where she teaches courses at the graduate and undergraduate level including Internet law. She is the co-author of a forthcoming textbook entitled *Internet Law and Policy*, and has written for various publications about legal issues in business.

Professor Hiller has been involved in research and service involving Internet regulatory issues for many years, including privacy and security and payment systems. She has served on several American Bar Association committees concerning these topics. She is the senior articles editor of the *Journal of Legal Studies Education*. Professor Hiller is a founding member and past director of the Center for Global Electronic Commerce at Virginia Tech, and past associate dean for Graduate and International Programs at the Pamplin College of Business.

Professor Hiller is a graduate of Virginia Tech (B.A. in 1978) and the University of Richmond (J.D. 1981).

Dr. France Bélanger is Director of the Center for Global Electronic Commerce and Assistant Professor of Information Systems in the Department of Accounting and Information Systems at Virginia Tech. Prior to her academic career, Dr. Bélanger held various technical, marketing, and managerial positions in large information systems and telecommunications corporations. She is also a consultant in electronic business and distance learning. Her research interests focus on the use of telecommunication technologies in organizations, in particular for distributed work arrangements, electronic commerce, and distance learning. Dr. Bélanger has presented her works at several national and international conferences, and has published in *Information Systems Research, Communications of the ACM, IEEE Transactions on Professional Communication, Information and Management, The Information Society,* and other information systems journals. She co-authored the books *Evaluation and Implementation of Distance Learning: Technologies, Tools and Techniques* (Idea Group Publishing, 2000), and *Foundations of E-Business Technologies* (John Wiley & Sons, forthcoming). Dr. Bélanger has a Ph.D. in information systems from the University of South Florida.

Key Contact Information

To contact the authors:

Janine S. Hiller
Center for Global Electronic Commerce
Pamplin College of Business
Virginia Polytechnic Institute and State University
3007 Pamplin
Blacksburg, VA 24061
(540) 231-7346

e-mail: jhiller@vt.edu

France Bélanger
Center for Global Electronic Commerce
Pamplin College of Business
Virginia Polytechnic Institute and State University
3007 Pamplin
Blacksburg, VA 24061
(540) 231-6720

e-mail: bélanger@vt.edu

ENDOWMENT REPORTS AVAILABLE

Innovations: Program Delivery

Managing Workfare: The Case of the Work Experience Program in the New York City Parks Department (June 1999)

Steven Cohen

New Tools for Improving Government Regulation: An Assessment of Emissions Trading and Other Market-Based Regulatory Tools (October 1999)

Gary C. Bryner

Religious Organizations, Anti-Poverty Relief, and Charitable Choice: A Feasibility Study of Faith-Based Welfare Reform in Mississippi (November 1999)

John P. Bartkowski
Helen A. Regis

Business Improvement Districts and Innovative Service Delivery (November 1999)

Jerry Mitchell

An Assessment of Brownfield Redevelopment Policies: The Michigan Experience (November 1999)

Richard C. Hula

San Diego County's Innovation Program: Using Competition and a Whole Lot More to Improve Public Services (January 2000)

William B. Eimicke

Innovation in the Administration of Public Airports (March 2000)

Scott E. Tarry

Entrepreneurial Government: Bureaucrats as Businesspeople (May 2000)

Anne Laurent

Rethinking U.S. Environmental Protection Policy: Management Challenges for a New Administration (November 2000)

Dennis A. Rondinelli

Innovations: Management

Credit Scoring and Loan Scoring: Tools for Improved Management of Federal Credit Programs (July 1999)

Thomas H. Stanton

Determining a Level Playing Field for Public-Private Competition (November 1999)

Lawrence L. Martin

Using Activity-Based Costing to Manage More Effectively (January 2000)

Michael H. Granof
David E. Platt
Igor Vaysman

Implementing State Contracts for Social Services: An Assessment of the Kansas Experience (May 2000)

Jocelyn M. Johnston
Barbara S. Romzek

Corporate Strategic Planning in Government: Lessons from the United States Air Force (November 2000)

Colin Campbell

The President's Management Council: An Important Management Innovation (December 2000)

Margaret L. Yao

Using Evaluation to Support Performance Management: A Guide for Federal Executives (January 2001)

Kathryn Newcomer
Mary Ann Scheirer

Managing for Outcomes: Milestone Contracting in Oklahoma (January 2001)

Peter Frumkin

Transforming Organizations

The Importance of Leadership: The Role of School Principals (September 1999)

Paul Teske
Mark Schneider

Leadership for Change: Case Studies in American Local Government (September 1999)

Robert B. Denhardt
Janet Vinzant Denhardt

Managing Decentralized Departments: The Case of the U.S. Department of Health and Human Services (October 1999)

Beryl A. Radin

Transforming Government: The Renewal and Revitalization of the Federal Emergency Management Agency (April 2000)

R. Steven Daniels
Carolyn L. Clark-Daniels

Transforming Government: Creating the New Defense Procurement System (April 2000)

Kimberly A. Harokopus

Trans-Atlantic Experiences in Health Reform: The United Kingdom's National Health Service and the United States Veterans Health Administration (May 2000)

Marilyn A. DeLuca

Transforming Government: The Revitalization of the Veterans Health Administration (June 2000)

Gary J. Young

The Challenge of Managing Across Boundaries: The Case of the Office of the Secretary in the U.S. Department of Health and Human Services (November 2000)

Beryl A. Radin

A Learning-Based Approach to Leading Change (December 2000)

Barry Sugarman

Creating a Culture of Innovation: 10 Lessons from America's Best Run City (January 2001)

Janet Vinzant Denhardt
Robert B. Denhardt

E-Government

Managing Telecommuting in the Federal Government: An Interim Report (June 2000)

Gina Vega
Louis Brennan

Using Virtual Teams to Manage Complex Projects: A Case Study of the Radioactive Waste Management Project (August 2000)

Samuel M. DeMarie

The Auction Model: How the Public Sector Can Leverage the Power of E-Commerce Through Dynamic Pricing (October 2000)

David C. Wyld

Supercharging the Employment Agency: An Investigation of the Use of Information and Communication Technology to Improve the Service of State Employment Agencies (December 2000)

Anthony M. Townsend

Assessing a State's Readiness for Global Electronic Commerce: Lessons from the Ohio Experience (January 2001)

J. Pari Sabety
Steven I. Gordon

Privacy Strategies for Electronic Government (January 2001)

Janine S. Hiller
France Bélanger

Revitalizing the Public Service

Results of the Government Leadership Survey: A 1999 Survey of Federal Executives (June 1999)

Mark A. Abramson
Steven A. Clyburn
Elizabeth Mercier

Profiles in Excellence: Conversations with the Best of America's Career Executive Service (November 1999)

Mark W. Huddleston

Leaders Growing Leaders: Preparing the Next Generation of Public Service Executives (May 2000)

Ray Blunt

Reflections on Mobility: Case Studies of Six Federal Executives (May 2000)

Michael D. Serlin

Toward a 21st Century Public Service: Reports from Four Forums (January 2001)

Mark A. Abramson, Editor

Becoming an Effective Political Executive: 7 Lessons from Experienced Appointees (January 2001)

Judith E. Michaels

To download or order a copy of these reports, visit the Endowment website at: endowment.pwcglobal.com

About PricewaterhouseCoopers

The Management Consulting Services practice of PricewaterhouseCoopers helps clients maximize their business performance by integrating strategic change, performance improvement and technology solutions. Through a worldwide network of skills and resources, consultants manage complex projects with global capabilities and local knowledge, from strategy through implementation. PricewaterhouseCoopers (www.pwcglobal.com) is the world's largest professional services organization. Drawing on the knowledge and skills of more than 150,000 people in 150 countries, we help our clients solve complex business problems and measurably enhance their ability to build value, manage risk and improve performance in an Internet-enabled world. PricewaterhouseCoopers refers to the member firms of the worldwide PricewaterhouseCoopers organization.

For additional information, contact:

Mark A. Abramson
Executive Director
The PricewaterhouseCoopers Endowment for
The Business of Government
1616 North Fort Myer Drive
Arlington, VA 22209

(703) 741-1077
fax: (703) 741-1076
e-mail: endowment@us.pwcglobal.com
website: endowment.pwcglobal.com

PRICEWATERHOUSECOOPERS

The PricewaterhouseCoopers Endowment for
The Business of Government

1616 North Fort Myer Drive
Arlington, VA 22209-3195

Bulk Rate
US Postage
PAID
Permit 1112
Merrifield, VA