Digital Government and Individual Privacy

Patrick R. Mullen
U.S. Government Accountability Office, Washington, DC, USA[1]

INTRODUCTION

Individual privacy is freedom from excessive intrusion by those seeking personal information about the individual. This allows the individual to choose the extent and circumstances under which personal information will be shared with others. A related concept, confidentiality, is a status accorded to information based on a decision, agreement, obligation, or duty. This status requires that the recipient of personal information must control disclosure. While privacy and confidentiality are concepts that can be applied to people in all societies, this article discusses them in relation to their treatment by the United States government, in particular with the advent of digital government. The concepts associated with digital government can also apply to non-Americans as well, but the discussion in this article is based on U.S. laws, documents, and relevant literature.

BACKGROUND

The growth of the Internet and digital government—that is, e-government—has dramatically increased the federal government's ability to collect, analyze, and disclose personal information about many private aspects of people's lives. Such information, once available only on paper to a limited number of people, is now instantly retrievable anywhere in the world by anyone with a computer and an Internet connection, including by hackers and firms specializing in selling information on individuals. At the same time as this dramatic increase in digital government, the level of trust in government has declined (Council for Excellence in Government, 2001); currently, many Americans perceive the government as a potential threat to individual privacy. Given these forces at work in American society, one should not be surprised to read the results of surveys that show privacy as a top concern of Americans in the 21st century. If Americans do not believe that the government is adequately protecting individual privacy, they may be less willing to provide the government with information. For example, most surveys by statistical agencies are voluntary, and even others that are mandatory, such as the decennial census and the American Community Survey, can suffer from underreporting by respondents. Such reluctance could compromise the ability of government to collect information necessary to develop, administer, and evaluate the impact of various policies and programs (Mullen, 2004).

FUTURE TRENDS

Generally speaking, e-government refers to the use of technology, particularly Web-based Internet applications, to enhance a specific agency's Web site, for access to and delivery of government information and services to individuals, businesses, and other organizations and government agencies. E-government has been seen as promising a wide range of benefits based largely on harnessing the power of the Internet to facilitate interconnections and information exchange between citizens and their government. A variety of actions have been taken in recent years to enhance the government's ability to realize the potential of e-government, culminating in the enactment of the E-Government Act of 2002 (Public Law 107-347), which includes provisions addressing everything from funding of e-government initiatives to measures for ensuring security and privacy. In addition to the E-Government Act, President George W. Bush designated e-government as one of five priorities in his management agenda for making the federal government more focused on citizens and results. The goals of President Bush's e-government initiative are summarized in Table 1.

Schelin (2003) discusses the rapid growth of e-government and provides an overview of the historical premises, theoretical constructs, and associated typologies of e-government that are a framework for understanding e-government and its potential benefits and related challenges. While the Internet opens new opportunities for streamlining processes and enhancing delivery of services, federal executives and managers must also be cognizant of the responsibilities and challenges that accompany these opportunities (Garson, 2003; Pavlichev & Garson, 2004; U.S. General Accounting Office, 2001a). Some of the responsibilities and challenges associated with managing e-government are summarized in Table 2.

Table 1. Goals of President Bush's e-government initiative

According to the President's management agenda, e-government is expected to:

- provide high-quality customer services regardless of whether the citizen contacts the agency by phone, in person, or on the Web;
- reduce the expense and difficulty of doing business with the government;
- cut government operating costs;
- provide citizens with readier access to government services;
- increase access for persons with disabilities to agency Web sites and e-government applications; and
- make government more transparent and accountable.

Table 2. Summary of e-government responsibilities and challenges

- Sustaining committed executive leadership
- Building effective e-government business cases
- Maintaining a focus on the individual
- Protecting individual privacy and confidentiality
- Implementing appropriate security controls
- Maintaining electronic records
- Maintaining a robust technical infrastructure
- Addressing IT human capital concerns
- Ensuring uniform service to the public
- Empowering citizens in democratic processes

PERSPECTIVES ON PRIVACY

In American society, there is an inherent tension between the desire for the free flow of information versus the concern for maintaining individual privacy. This tension is captured in various congressional statements, included in legislation as well as in executive branch guidance to agencies, which explain how to carry out their seemingly conflicting responsibilities under the law. For example, in passing the Paperwork Reduction Act of 1995, the Senate Governmental Affairs Committee (1995) noted that "information obtained by government is a valuable and useful resource to government and society, if managed in a coordinated and systematic manner." The committee also noted the importance of the free flow of information:

"The advent of the electronic information age presents new opportunities and obligations of the Federal government as it strives to fulfill its continuing responsibility to make government information accessible to the American public. The legislation meets this need by providing for improved dissemination of government information to the public, particularly in electronic formats."

However, these same technological trends also raise concerns about information privacy. As Congress stated in passing the Privacy Act (1974):

"…the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur for any collection, maintenance, use, or dissemination of personal information."

While the Privacy Act is the primary law regulating the federal government's collection and maintenance of personal information, the legislative intent has been clarified with subsequent Office of Management and Budget (OMB) guidance to federal agencies. OMB's circular on "The Management of Federal Information Resources" (Circular A-130) also captures the balance between the free flow of information versus individual privacy (U.S. Office of Management and Budget, 2000), addressing (1) the need for agency Web sites to post clear and easily accessed privacy policies and (2) federal agency use of Internet cookies—short strings of text sent from a Web server to a Web browser when the browser accesses a Web page—which poses privacy risks because the data contained in persistent cookies may be linked to individuals after the fact (U.S. General Accounting Office, 2001b). In addition, the Federal Trade Commission (FTC) has issued four Fair Information Principles governing online privacy at commercial Web sites. These principles can be used as criteria to assess federal agency Web sites (U.S. General Accounting Office, 2000; Center for Democracy and Technology, 1999). The principles are included in Table 3.

PROTECTING INDIVIDUAL PRIVACY

Individual privacy is closely related to data confidentiality and security (Boruch & Cecil, 1979; Duncan, Jabine &