6

Managing Information Privacy and Information Access in the Public Sector

by
George T. Duncan
H. John Heinz III School of Public
Policy and Management
Carnegie Mellon University

Government agencies collect and disseminate data that bear on the most important issues of public interest. Advances in information technology, particularly the Internet, have multiplied the tension between demands for evermore comprehensive databases and demands for the shelter of privacy. In mediating between these two conflicting demands, agencies must address a host of difficult problems. These include providing access to information while protecting confidentiality, coping with health information databases, and ensuring consistency with international standards. The policies of agencies are determined by what is right for them to do, what works for them, and what they are required to do by law. They must interpret and respect the ethical imperatives of democratic accountability, constitutional empowerment, and individual autonomy. They must keep pace with technological developments by developing effective measures for making information available to a broad range of users. They must both abide by the mandates of legislation and participate in the process of developing new legislation that is responsive to changes that affect their domain. In managing confidentiality and data access functions, agencies have two basic tools: techniques for disclosure limitation through restricted data and administrative procedures through restricted access. The technical procedures for disclosure limitation involve a range of mathematical and statistical tools. The administrative procedures can be implemented through a variety of institu-

tional mechanisms, ranging from privacy advocates, through internal privacy review boards, to a data and access protection commission

The Tension Between Private Lives and Public Policies

An Environmental Scan

In its normal activities, the public sector captures enormous amounts of data, stores it in very large databases, analyzes some of it, and disseminates information products to individuals, governments, businesses, and other organizations. Much of these data are obtained directly from respondents in surveys and censuses or through building systems of administrative records based on a variety of citizen interactions with government. Surveys include:

- Face-to-face interviews, as with the National Longitudinal Surveys of Young Women conducted by the Bureau of Labor Statistics
- Telephone surveys, as with the Behavioral Risk Factor Surveillance System conducted by the Center for Disease Control, which estimates current cigarette smoking and use of smokeless tobacco
- Mail-back responses (including electronic mail), as with the reactions to their web site obtained by Inland Revenue of the Government of New Zealand (see http://www.ird.govt.nz/survey.htm).

Administrative records include:

- Employer-furnished data, as with Social Security Administration earnings records
- Licensing data, as with state Departments of Motor Vehicles and local building permits
- Individual and firm submitted data, as with Internal Revenue Service tax returns.

The Internet has accelerated the demand for access to government information services, primarily by broadening the range of potential data users. Access demand is in commensurate tension to concerns about privacy and confidentiality. The National Science Foundation in its Digital Government program announcement (NSF 1998), affirms, "Given the inexorable progress toward faster computer micro-processors, greater network bandwidth, and expanded storage and computing power at the desktop, citizens will expect a government that responds quickly and accurately while ensuring privacy." This article focuses on ways the public sector can resolve the growing tension between the demand for government data and concerns for privacy protection.

Government databases are rich in information and have evident practical utility for planning, marketing, and research. Still, many would-be users complain they cannot obtain the data they need, often thwarted by confidentiality concerns (Smith 1991). On the other hand, privacy advocates warn of the dangers of unfettered data capture and dissemination. Their arguments are ethically based. "Individuals in the Western world are increasingly subject to surveillance through the use of data bases in the public and private sectors, and these developments have negative implications for the quality of life in our societies and for the protection of human rights." (Flaherty

Related Content

Netnography: A Review of Its Application in Social Media and Digital Government Research
Inderjeet Kaur, Diptanshu Gaur, Ashwani Kumarand Fatmah Mohmmad H. Alatawi (2021). *International Journal of Electronic Government Research (pp. 63-83).*
www.irma-international.org/article/netnography/289356

Voter Information Web Sites
A. Edwards (2007). *Encyclopedia of Digital Government (pp. 1623-1628).*
www.irma-international.org/chapter/voter-information-web-sites/11724

E-Government Implementation Perspective: Setting Objective and Strategy
Mahmud Akhter Shareef, Vinod Kumar, Uma Kumar, Abdul Hannan Chowdhuryand Subhas C. Misra (2010). *International Journal of Electronic Government Research (pp. 59-77).*
www.irma-international.org/article/government-implementation-perspective/38964

Requirements on Cross-Agency Processes in E-Government: The Need for Reference Model
Jeffrey Gortmaker, Marijn Janssenand Rene W. Wagenaar (2008). *Electronic Government: Concepts, Methodologies, Tools, and Applications (pp. 2363-2375).*
www.irma-international.org/chapter/requirements-cross-agency-processes-government/9863

Artificial Intelligence Adoption for E-Government: Analysis of Enablers in an Emerging Economy
Abdulla H. M. A. Fetais, Mohd Nishat Faisal, Lamay Bin Sabirand Bader Al Esmael (2022). *International Journal of Electronic Government Research (pp. 1-21).*
www.irma-international.org/article/artificial-intelligence-adoption-for-e-government/300773