E–Government Databases

Catherine Horiuchi
Seattle University, USA

INTRODUCTION

The new face of government is electronic. Prior to the development of e-government, adoption of small-scale computing and networking in homes and businesses created the world of e-business, where computer technologies mediate transactions once performed face-to-face. Through the use of computers large and small, companies reduce costs, standardize performance, extend hours of service, and increase the range of products available to consumers. These same technological advances create opportunities for governments to improve their capacity to meet growing public service mandates. Tasks that formerly required a trip to city hall can be accomplished remotely. Government employees can post answers to frequently asked questions online, and citizens can submit complex questions through the same electronic mail (e-mail) systems already used at home and in businesses. This developing e-government increases the number and complexity of electronic databases that must be managed according to the roles information plays in government operations.

BACKGROUND

E-government has been defined as the application of e-business technologies and strategies to government organizations, the delivery of local government service through electronic means, and a method to enhance the access to and delivery of its services to benefit citizens. E-government is envisioned to be “a tool that facilitates creation of public value” (United Nations, 2003). In its survey of member states, the UN found 173 of 191 members have government Web sites, offering at minimum government information and some measure of service. Common capabilities of governmental Web sites include ability to download government forms and access information on a region or local services (Swartz, 2004). The United States has the largest number of citizens with Internet-connected computers at home and the most developed network infrastructure, resulting in the greatest amount of information and number of services and products available online. Even so, information technology process adaptations for government services are rudimentary, and many citizens do not have the ability to access their government remotely.

Less visibly, e-government adoption is steadily increasing connections made through the Internet between public agencies and private networks. This connectivity creates computer-to-computer interfaces between multiple databases. Some connections include Web-enabled access to decades-old data structures stored on traditional mainframe systems. Other systems use new databases built or bought from proprietary third parties. A third type of major database project ports data from older systems into new Web-enabled models. Functional requirements determine the database management properties needed by each data system.

E-GOVERNMENT DATA SYSTEMS

Technology utilization and diffusion of technological processes are increasingly important in managing the “hollow state” (Milward & Provan, 2000). This model of governance is desirable because it allows for greater flexibility in government budgeting and operations. A systematic contracting process creates price competition and encourages fresh approaches to social services, but also requires coordination of information and applications to exchange data securely between the service providers and the government agency. To facilitate this, e-government has adopted structuring concepts first developed in commercial sectors as business-to-business (B2B) and business-to-consumer (B2C) applications. Process re-engineering in government is transforming these concepts into government-to-business, government-to-citizen, and government-to-government constructs with parallel acronyms G2B, G2C, and G2G, respectively. Each of these models creates its own service and reliability profile. Diffusion of data is an essential element of these business processes adopted by government (Bajaj & Sudha, 2003), resulting in large data sets shared among technology project partners.

Sometimes, these diffusions go awry because government is not like business in fundamental ways (Allison, 1980) that make government databases more comprehensive and at the same time more vulnerable to data dissemination contrary to established procedures. In one high
profile case, over five million traveler records were provided by an airline to a government contractor working on a Pentagon data mining and profiling project (Carey & Power, 2003), contrary to the airline’s privacy policy. The data were cross-referenced to other demographic data available from another firm. The expanded data set was then used in a paper that was presented at a technology conference and posted briefly on the conference Web site. In a similar case of unauthorized data exchange, an airline transferred 1.2 million records—names, addresses, phone numbers, and credit-card information—to multiple private firms competing for government contracts. This was not reported for nearly two years (McCartney & Schatz, 2004). The U.S. government’s Computer-Assisted Passenger Prescreening System (CAPPS II), intended solely as a screening tool, was cancelled in response to the public outcry over multiple incidents of unauthorized release of data (Alonso-Zaldivar, 2004). The misuse occurred despite assurances by the government that travel data would be protected from precisely this type of diffusion and dissemination, that “information will only be kept for a short period after completion of the travel itinerary, and then it will be permanently destroyed” (Department of Homeland Security, 2003a, p. 1) and stored “at a TSA secure facility” (Department of Homeland Security, 2003b, p. 16).

Models developed for commercial enterprises weakly map to specific requirements of governmental systems. The myriad roles of government result in unique system requirements. Table 1 lists some of the e-government applications already in operation in at least some jurisdictions.

The range in requirements can be highlighted by a brief comparison of two very different applications and properties of the databases they require. In the adoption of e-voting, governments are replacing paper ballots with touch-screen terminals as the voter interface, using machine technology for tabulating the votes and aggregating election results. Once an election is certified, the database can be reinitialized for the next election. For parcel and tax records, information that has been kept for a short period after completion of the travel itinerary, and then it will be permanently destroyed. A similar case of unauthorized data exchange, an airline transferred 1.2 million records—names, addresses, phone numbers, and credit-card information—to multiple private firms competing for government contracts. This was not reported for nearly two years. The U.S. government’s Computer-Assisted Passenger Prescreening System (CAPPS II), intended solely as a screening tool, was cancelled in response to the public outcry over multiple incidents of unauthorized release of data. The misuse occurred despite assurances by the government that travel data would be protected from precisely this type of diffusion and dissemination, that “information will only be kept for a short period after completion of the travel itinerary, and then it will be permanently destroyed.”

The contested U.S. presidential election involved the unlikely scenario where the margin of votes for victory in several states appeared smaller than the margin of error for the semi-automated tools that tabulated votes. This resulted in a challenge to the validity of the election results. The public manager must develop information strategy and management skills better suited to the adoption of advanced technologies. These new skills involve system security models, measuring system efficacy, utilizing tools for archival of public records, and managing information across system life cycles that vary widely, put into a public service context. Public managers have not developed these skills at the same rate that they have implemented new technologies or undertaken large projects, contributing to the high failure rate of public sector technology initiatives. These failures range from high-profile project abandonment to an assessment of low value for cost, such as the 1994 assessment that $200 billion in federal expenditures over 12 years created little discernable benefit.

**ELECTRONIC VOTING**

Beginning in the 1990s with the development of easily understood Internet browser applications and the widespread penetration of personal computers into households, governments have sought to facilitate access and services through this familiar interface. The introduction of modern technology to one fundamental government activity—voting—has drawn special attention both for its potential to accurately and rapidly count votes and for the specific problems associated with the data collected.

Voting machine technology has gradually been modernized. The original paper ballots have been replaced in varying districts. First developed were mechanical lever machines, then punch cards either supplied with hole punchers or pre-perforated. Optical scanners read cards with ovals or squares that have been filled in by pencil or pen. The most recent introduction incorporates personal computer technology and networks to create computer-based electronic voting (e-voting) systems. All but the latest technologies have been in active use for decades. In the 1996 U.S. presidential election, approximately 2% of the votes were cast on paper ballots, 21% on mechanical lever systems, 37% on punched cards, 25% on optical cards, and nearly 8% on e-voting machines. Despite ongoing efforts to modernize voting technologies to simplify voting and reduce errors, an election dispute in 2000 began a public debate on computers, databases, networks, and voting.

The contested U.S. presidential election involved the unlikely scenario where the margin of votes for victory in several states appeared smaller than the margin of error for the semi-automated tools that tabulated votes. This resulted in a challenge to the validity of the election results. The public manager must develop information strategy and management skills better suited to the adoption of advanced technologies. These new skills involve system security models, measuring system efficacy, utilizing tools for archival of public records, and managing information across system life cycles that vary widely, put into a public service context. Public managers have not developed these skills at the same rate that they have implemented new technologies or undertaken large projects, contributing to the high failure rate of public sector technology initiatives. These failures range from high-profile project abandonment to an assessment of low value for cost, such as the 1994 assessment that $200 billion in federal expenditures over 12 years created little discernable benefit.

### Table 1. E-government public services applications

<table>
<thead>
<tr>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational Web site (online brochure)</td>
</tr>
<tr>
<td>Permitting</td>
</tr>
<tr>
<td>Webcasting of meetings</td>
</tr>
<tr>
<td>License renewals</td>
</tr>
<tr>
<td>Records requests</td>
</tr>
<tr>
<td>E-voting</td>
</tr>
</tbody>
</table>