Chapter 6.7
E-Government, Security, and Cyber-Privacy:
Individual Rights vs. Government Responsibility

Ross Wolf
University of Central Florida, USA

Ronnie Korosec
University of Central Florida, USA

ABSTRACT

E-government involves governments at all levels using advanced technology and communication tools to provide services, allow for transactions, and respond to citizen's needs and requests. This on-line version of government, which is designed to enhance efficiency and improve operations, relies heavily on a network of data structures that are currently in place. While much has been written about e-government, few studies exist that link the concepts of e-government and security with individual rights and government responsibility. Now more than ever, progressive changes in technology allow public and private sector entities to routinely collect, store, and disseminate large files of personal information about the citizens and clients they interact with. The power associated with the magnitude of this information requires great responsibility and accountability. This chapter is a beginning point to discuss how governments in the United States attempt to maintain secure fortresses of data, limit the dissemination of sensitive information to unauthorized parties, and ensure on line privacy for citizens.

DOI: 10.4018/978-1-61350-323-2.ch6.7

INTRODUCTION

During the last decade, governments have increasingly embraced electronic technologies as a means to provide more efficient points of contact for citizens to access government information and services on line, as well as to collect necessary data and information about the citizens and communities they serve. While the expansion of electronic government services (or 'e-government') has resulted in various cost savings and service improvements for citizens and administrators, it has also created several challenges. Many citizens may appreciate the ease in accessing city council meeting minutes, reviewing police reports, analyzing property records, or applying for government jobs on line, but they may not realize that potentially sensitive information about them may be collected, stored, and accessed on line or through other media used in elaborate e-government networks. Although much of this information is readily available through the Freedom of Information Act (FOIA) and state open government laws, some citizens have argued that the scope of this information and the potential for it to fall into the hands of those who will use it for negative gains presents too great of a threat to their privacy.

While the US Constitution does not specifically mention individual rights to privacy, there are inherent references to it in the 3rd, 4th, and 5th Amendments. The forth amendment is perhaps most germane to this discussion, as it states (with emphasis added):

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (The Constitution of the United States of America).

This has been interpreted broadly to mean that citizens have the right to keep sensitive information about themselves private, and also to limit the distribution of that information. The extent of, need for, and use of data by governments creates a quandary for them and their affected citizens. Government agencies collect personal information for a variety of reasons. However, as individual data becomes more and more readily available at the click of a mouse, citizens have raised concerns over the amount of data that is available to anyone with a computer, an internet connection, and an interest. Seen as one of the greatest accomplishments of the modern era, the internet is also responsible for most concerns about the privacy of personal information (Burgunder, 2007). Concerns over keeping on line information secure, or 'cyber-privacy' are not new. Americans have long been concerned with the government's collection of data, but the availability of information today through government-run or government-partnered websites has greatly amplified suspicion. Most governments rely on freedom of information or open government laws that insist that certain information be made public. There are few laws that shield information from public scrutiny.

As the internet has become the chosen means for municipal, local, and state governments to post information and allow for instant access, it has also simplified record searching, giving "individuals the opportunity to easily access enormous banks of information that once were available only to the most dedicated information sleuths" (Burgunder, 2007, p. 585). Real estate records, mortgage information, bankruptcy filings, home phone numbers and addresses, divorce records, and criminal charges are just some of the pieces of information available through government agencies. Before the internet, the fact that government agencies collected certain data and allowed public review of it upon request was of little concern to most citizens. In order for anyone to access data they would have to drive to a government building, locate the right person, often make a written request for information, and pay a