
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 online 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)._