Chapter 10
Privacy and Public Access in the Light of E-Government: The Case of Sweden

Elin Palm
The Royal Institute of Technology, Sweden

Misse Wester
The Royal Institute of Technology, Sweden

ABSTRACT

This chapter addresses the competing interests of privacy versus public access to information. The chapter explores the collective and individual value of privacy and public access in a manner that considers information at the macrosocial and macroethical level. By using Sweden as a case study, we exemplify the classic and irresolvable tension between issues of information availability and confidentiality, integrity, and privacy. Given that privacy and public access interests will constantly need to be rebalanced, we present the views of government officials due to their unique role in implementing this balance. We conclude with an analysis of the reasonableness of this conduct.

INTRODUCTION

Modern society is, to a large extent, dependent on services and applications based on Information and Communication Technology (ICT). The focus of this chapter is online services that governments offer citizens, which is sometimes described in terms of a shift to a "paperless government". One of the hopes for e-Government is that it will, if correctly used, increase transparency and civic involvement. This is an important aspiration. As a result of the European Union's (EU) e-Government strategy of April 2006, several programmes have been launched to promote a more efficient and easily accessible digital government. The extent to which individual member states offer on-line services, however, vary (UN, 2008).

In Sweden, ranked third on the United Nations' 2008 e-Government Readiness Index, a long-standing governmental goal has been to create the "24 hours authority" – an electronic service available 24 hours a day, 7 days a week, providing Swedish citizens access to public services

DOI: 10.4018/978-1-61692-245-0.ch010

and contact with all government authorities and agencies at all times. Although the encompassing e-Government has not been launched as planned, a significant number of governmental services are currently made available on-line. Increasingly, Swedish citizens rely on e-services for tax issues, pensions, parents' allowance and health insurance.

Although e-Government is seen as desirable for improving access to services, transparency, and civic involvement, projects aimed at establishing e-Government are typically considered difficult and include a large amount of risk (Heeks, 2006; Heeks & Stanforth, 2007). Most e-services are based on ICT and share the general vulnerabilities of the Internet infrastructure. That is, ICT enables new forms of classical crimes like fraud, novel crimes like hacking and identity theft, and controversial practices like data mining (Cavoukian, 1998; Tavani, 1999). The expanding field of on-line governmental service implies that an increasing amount of personal information is collected and transferred via channels that may be difficult to secure. Information security concerns, such as confidentiality, integrity, availability, and reliability of data pose serious challenges. The emerging e-service society increases the need for well functioning information security – both system security and security of personal data (Brey, 2007). Data protection requires both robust technical systems to protect the data and awareness of proper and ethically defensible ways of handling the information to be collected and processed.

The true challenge, as we see it, is not in ensuring access to e-services or in guaranteeing security. Rather, the challenge is finding and maintaining a proper balance between the social costs and benefits when securing e-governmental services and safeguarding the privacy of citizens. It is widely recognized in the field of information assurance and security that the most significant challenges are in implementation where information assurance and security must integrate technical, organizational, and policy countermeasures. Successful integration of technical and nontechnical information assurance and security countermeasures hinges on the knowledge levels and attitudes of decision makers. In this chapter we explore the issue of balance from an ethical perspective by focusing on the attitudes towards e-Government, privacy, and data protection among representatives of six Swedish governmental agencies. Those interviewed are professionals dealing with the security and privacy implications of e-services. Drawing from their expreriences we discuss the ethical aspects of reasonable use, access to, and control over personal data as, well as the task of balancing these interests.

The chapter is organized as follows. The next section provides a background to the discussion on ethical aspects of e-Government. Section three discusses benefits and risks attached to e-services and e-Government. Section four provides a brief inventory of prevailing privacy protection policies and legislation. Section five offers a philosophical basis for privacy protection. Section six discusses potential conflicts between privacy and data protection on the one hand, and the principles of transparency and public access to official documents on the other hand. Section seven analyzes conflicts between public access and privacy in relation to the findings from the empirical study on attitudes in government agencies. Section eight indicates future research directions. Section nine summarizes and concludes the issues discussed in this chapter.

BACKGROUND

e-Government can be defined as ICT-based services for public administration on a national or international level. As noted above, the European Union is advocating the development of e-Government. The 2006 Action Plan on e-Government requires EU Member States to commit themselves to inclusive e-Government objectives to: