Chapter 5.33
Social Issues of Trust and Digital Government

Stephen Marsh
National Research Council of Canada, Canada

Andrew S. Patrick
National Research Council of Canada, Canada

Pamela Briggs
Northumbria University, UK

INTRODUCTION

Building any online system or service that people will trust is a significant challenge. For example, consumers sometimes avoid e-commerce services over fears about their security and privacy. As a result, much research has been done to determine factors that affect users' trust of e-commerce services (e.g., Egger, 2001; Friedman, Khan, & Howe, 2000; Riegelsberger & Sasse, 2001). Building trustable e-government services, however, presents a significantly greater challenge than e-commerce services for a number of reasons. First, government services are often covered by privacy protection legislation that may not apply to commercial services, so they will be subject to a higher level of scrutiny. Second, the nature of the information involved in an e-government transaction may be more sensitive than the information involved in a commercial transaction (Adams, 1999). Third, the nature of the information receiver is different in an e-government context (Adams, 1999). Some personal information, such as supermarket spending habits, might be relatively benign in an e-commerce situation, such as a loyalty program (supermarket points, or Air Miles, for instance), but other information such as medical records would be considered very sensitive if shared amongst all government agencies. Fourth, the consequences of a breach of privacy may be much larger in an e-government context, where, for example, premature release of economic data might have a profound effect on stock markets, affecting millions of investors (National Research Council, 2002).

E-government services also involve significant privacy and security challenges because the traditional trade-offs of risks and costs cannot be applied as they can in business. In business contexts it is usually impossible to reduce the risks, for example of unauthorized access to information, or loss of or corruption of personal information, to zero and managers often have to trade-off acceptable risks against increasing costs. In the e-government context, because of the nature of the information and the high publicity, no violations of security or privacy can be considered acceptable (National Research Council, 2002). Although zero risk may be impossible to achieve, it is vital to target this ideal in an e-government service. In addition, government departments are often the major source of materials used to identify and authenticate individuals. Identification documents such as driver's licenses and passports are issued by government agencies, so any breach in the security of these agencies can lead to significant problems. Identity theft is a growing problem worldwide, and e-government services that issue identification documents must be especially vigilant to protect against identity theft (National Research Council, 2002). Another significant challenge for e-government systems is protecting the privacy of individuals who traditionally have maintained multiple identities when interacting with the government (National Research Council, 2002). Today, a driver's license is used when operating an automobile, a tax account number is used during financial transactions, while a government health card is used when seeking health services. With the implementation and use of e-government services it becomes possible to match these separate identities in a manner that was not being done before, and this could lead to new privacy concerns.

BACKGROUND

Trust is a cognitive process and behavior that people use every day to make decisions, reassure themselves, judge information, confer authority, take or assign responsibility under uncertainty, and simply to get out of bed in the morning (Luhmann, 1979). It's one of the building blocks of society (Bok, 1978; Misztal, 1996) and it is necessary for effective day-to-day cooperation. It is worth noting that the decline (or otherwise) of public trust in government is not necessarily universal, and is a phenomenon worth much further study. That said, trust in some governments has been studied extensively, particularly with regards to the decline of trust in public institutions (for example, see Thomas, 1998; Uslaner, 2001), as well as the apparent increase in trust in government in the U.S. post-September 11th (Chanley, 2002). As well, the link between political and social trust has been extensively studied (see for example, Newton, 2001).

Recently, as evidenced by this volume, there has been an upsurge in bringing government closer to the people by making services, ideas, decision makers, and procedures available to people using information and communication technologies (ICTs). One of the laudable ideals of this work is that, by increasing citizen participation in government, the crisis of confidence (trust) can be answered and to some extent reversed. That is, if citizens have more of a say in running their country than an election every few years, they will feel more connected with government, and thus trust it more (e.g., Advisory Committee to the Congressional Internet Caucus, 2001).

Trust is a multidimensional concept and addressing it completely would result in a book on its own. Here we will introduce trust issues in digital government by briefly defining what trust actually is, both in terms of social trust and trust in the digital sphere, then what digital government projects can do that address trust issues, pointing out some of the pitfalls and problems associated with the work.

DEFINING TRUST

Trust, although not always a mainstream research topic (Misztal, 1996), has in recent years become much more fashionable. Ironically, this is in large