Trust in Digital Government

Neil C. Rowe
U.S. Naval Postgraduate School, USA

INTRODUCTION

The concept of trust in organizations has been an important area of recent research in sociology and management science (Sztompka, 1999). Trust is positive expectations of positive actions by others, and is important to well-functioning organizations of all sorts. Trust facilitates the effectiveness of government. A focus on trust leads to a more humanistic view of individuals within organizations than that of the traditional managerial psychology of humans solely as input-output devices whose performance must be monitored and measured.

New technology changes the form of government operations. So it is natural to ask how trust is affected by the advent of the technologies and practices of digital government, as it is affected by online security practices (Friedman, Kahn, & Howe, 2000). On the one hand, digital government should be more efficient government, and people trust more in well-run, efficient processes. On the other hand, digital government could enable governments to evade responsibility for their actions by imposing new barriers to citizens, restricting access to information more, falsifying information more easily, and providing a new set of excuses for inefficiency. Some extremists (Postman, 1993) claim that most technology cannot be trusted, but few people agree. So the issue needs to be examined at length.

BACKGROUND

Sztompka (1999) provides a detailed analysis of trust relationships. He defines trust as "a bet on the future contingent actions of others" and enumerates six major factors supporting it: (1) reputation, (2) performance, (3) appearance, (4) accountability, (5) precommitment, and (6) contextual facilitation. Of these factors, reputation is not much influenced by whether government is digital or not. Performance and accountability are supported by virtually any digital government as well as government: Past performance of government (demonstrating that procedures are being followed) and lines of accountability (indicating that recourse is available for fixing problems) are almost always present. But digital government can improve performance and accountability by exploiting its ability to store extensive documentation. For instance, digital government can keep records (while removing identifying information to maintain privacy) to demonstrate that citizens are being treated fairly and equally. They can also track citizen interactions and requests to show that procedures are functioning properly.

Appearance is related to the user friendliness of digital government, and this can be ensured by good human interface design for the software, with phone numbers and email addresses of human contacts provided in case of problems. Precommitment (fulfilling initial steps to build trust in completing a full promise) can be accomplished in digital government by offering receipts, certificates, and other documentation at milestones while providing a service. Finally, contextual facilitation is the "culture of trust" cultivated by a government by treatment of its citizens, and is only indirectly related to digital government through its performance.

Sztompka also distinguishes between instrumental trust (related to specific goals), axiological (based on moral expectations), and fiduciary (based on legal or quasi-legal obligations). Government is generally a means to the ends of its citizens, rarely makes moral claims, but does fulfill legal obligations. Thus it concerns instrumental and fiduciary trust, the latter in regard to laws and the former in regard to everything else. (Hardin, 2002) points out other important differences between trust in government and trust in people, and suggests that government cannot actively seek the trust of its citizens but can only gain trust by acting consistently in a trustworthy manner. Levi and Stocker (2000) point out other important kinds of trust involved in citizen-government relations.

ACCESSIBILITY OF DIGITAL GOVERNMENT

Now let us consider some specifics of trust in digital government. Digital government usually strives to increase accessibility of the government to the citizens, and this will increase trust in the government by Sztompka's factors of appearance and performance. Digital government provides good ways for government to get public feedback with surveys, complaint forms, and online discus-

sion groups. But this requires some effort by the government; a digital government designed only for efficiency may function as a "screen" keeping government officials more distant from the people, thereby decreasing trust.

Even when digital government is accessible, not all citizens may have equal access to it. A social and cultural gulf separates the computer literate and the computer illiterate because of the necessary investment in technology (Cronin, 1995). The computer illiterate are feeling increasingly disenfranchised, and this exacerbates their mistrust of a government that uses digital government technology. So it is essential that government provide technological support for access to digital government by all citizens. This could take the form of free public access devices at dispersed locations, or subsidies for the purchase of devices and software necessary to use digital government. It should also include free training in their use, because not all technology can be designed to be usable without training. Without such steps to make digital government accessible to most of a society, distrust of government will increase regardless of its efficiency.

SECRECY IN DIGITAL GOVERNMENT

All governments keep secrets to protect themselves from exploitation by other governments and to preserve the privacy of their citizens (Yu, Kundur, & Lin, 2001). Information technology can help protect secrets. For instance, messages encrypted with today's strong encryption methods cannot be deciphered without the key no matter what incentives are offered. Other technological developments like cryptographic protocols, security kernels of operating systems, and firewalls are also helping secrecy and protecting privacy, and generally promoting trust in government.

But governments that want to keep unnecessary secrets will also find this technology helpful, and this can hurt trust in regard to Sztompka's issues of appearance and accountability. This is a political issue, however, and citizens may have different ideas than their government does about what should be kept secret (Theoharis, 1998). Governments need to legitimize themselves, and secrecy erodes legitimacy. If taxpayers cannot see what their taxes are being spent on, or militaries fail to protect a country despite their secrecy, dissatisfaction grows. Economic downturns or unpopular wars may then cause serious political stresses, and can even destroy a government, as happened in Argentina in the 1980s. The number of secrets kept by the United States government continues to increase without much justification, damaging citizen trust.

Secrecy includes prevention of correlating disparate pieces of non-secret information to infer secrets. For instance, knowledge of the average salary of female employees in a department can be combined with knowledge there is only one female employee in the department to infer her salary. However, these problems are well known by statistical agencies, and automatic checks can be made before releasing correlatable information (Adam & Worthmann, 1989).

DELIBERATE DECEPTION IN DIGITAL GOVERNMENT

Politicians lie and equivocate on many occasions since protecting secrets and pleasing large numbers of people often requires it (Eckman, 2001; Nyberg, 1993). This accounts for some of the low trust that citizens have in governments. Thus it is important for digital government to maintain high standards of truth telling to avoid being associated with the poor reputation of politicians (and losing trust on Sztompka's factors of reputation and performance). One important principle is that digital government should mostly record and report matters of fact. Exceptions must be made for discussions and public comments on matters of policy, but even these can be made more trustworthy by ideas such as linking statements in a discussion to the raw data supporting them. World Wide Web technology makes it easier to provide such links.

A reason to be very cautious about deception by governments is that trust is subject to different laws than distrust. Josang (2001) argues that trust can decrease quickly with experience but distrust decreases much more slowly, and this has been confirmed in experiments (Rowe, 2004). This is because actions that create distrust tend to be hard to interpret as accidental. Thus a few incidents of deception (or even half deceptions) can ruin the trustworthiness that a government has taken years to build. But easy online access to validated information should reduce the ability and desire of governments to lie about matters of fact, reducing the total amount of lying that they do. And if a government that tries to limit access to important information, or lies about possessing it, it can be seen as almost as bad as if it lied about it in the first place, as citizens become familiar with the capabilities of digital government.

Another issue is that third parties besides a government and its citizens could use digital government technology for their own deceptions. For instance, vendors could insert advertising in the software they supply to a government, or trespassers could post false information on government Web pages. Such events would lower