Trust in digital government

Neil C. Rowe
Cebrowski Institute
U.S. Naval Postgraduate School
Monterey, CA 93943 USA

(This is a chapter in the *Encyclopedia of Digital Government*, ed. A.-V. Anttiroiko & M. Malkia, Hershey, PA, USA: The Idea Group, 2006.)

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 & 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 discussion 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 public trust in the government. So digital government must enforce software standards and implement good information-security practices.

AUDITING

Every legitimate government must also provide safeguards to prevent secrecy from being exploited for personal or political advantage. For instance, secrecy should not be permitted to enable embezzlement, awards of contracts to relatives of government employees, or a campaign of harassment against political enemies. Audits are one way to prevent this (Mercuri, 2003). These are independent analyses of the secret data by accountants, regulators, lawyers, and other purportedly independent evaluators to confirm that policy and laws are being obeyed. Computer software is essential to auditing as it can systematically check all the details. Software can also check for bugs and loopholes, either inadvertent or deliberate, that could permit policy violations or crime (Prins, 2002). With automatic auditing, digital government can in fact be made more trustworthy than traditional government.

Auditing requires recording all changes and attestations for a key document such as a budget with indications of who made them and when; computers can easily record such information. Then if there are discrepancies, blame can be localized, and this supports Sztompka?s trust factor of accountability. Such controls necessarily increase bureaucracy in government, but bureaucracy is a price that must be paid for a trustworthy government (Wilson, 2000). Bureaucracy has an additional benefit in increasing the reciprocal trust that government employees have in citizens, since it limits citizen interactions to a narrower set of activities and this can reduce the stress on government employees.

Mandated disclosure is often coupled to auditing; it can reduce the amount of secrecy used by a government and improve its legitimacy through accountability for decisions. For instance, departments can be required to disclose how they spent their budgets. Mandated disclosure can occur after a time limit. For instance, classified information in the United States must be disclosed after a period of time when it cannot compromise ongoing activities. While intelligence agencies may grumble about it, it is usually beneficial for trust in government to reveal fifty-year-old information.

AUTHENTICATION

Authentication is an accountability technique related to auditing, and includes methods for verifying the integrity of information and the identity of people (Smith, 2001). Authentication can confirm that digital documents are unmodified, which is important since it is so easy to change them. Authentication can also prove that software (including auditing software) has not been tampered with, confirming that no viruses, worms, or other "Trojan horses" have been inserted. Authentication of digital data uses methods of cryptography and "digital signatures"; public-key cryptography is particularly useful because it can be used either to encrypt or to authenticate. Effective authentication methods prevent signatures from being copied from one document to another by making the signature a complicated function of the contents and date of the document.

Authentication can thus prove the author of a document, which prevents forgeries as well as later disavowal of authentic documents; this supports strong accountability. Authentication also can prove that a document in a sequence is missing, if one encrypts pointers to the previous and subsequent documents for each document. It can also identify sources of information leaks, by using steganography to embed unique hidden messages in each copy of a document, as in the pattern of spaces or line lengths (Wayner, 2002). Authentication and auditing are critical in providing trust in electronic voting (Kofler, Krimmer, & Prosser, 2003).

Authentication also helps preserve privacy of citizens by requiring credentials to access data. If a government site permits unauthorized people to read private personal information of citizens like credit-card numbers, addresses, and birth dates, it will quickly lose the trust of its citizens. Even less obviously private data like who has visited a government site should be restricted to maintain good public trust. So access to citizen data should require secure authentication permitting access of a very small number of

government employees.

But authentication on computer systems only works when one can trust the computer systems on which it is done. This requires that the operating system of the computer is free of security flaws, a challenge for the popular operating systems of Windows and Linux for which security flaws are being discovered all the time. An older and well-debugged version of an operating system can be selected, a very safe operating system with "security kernels" can be used, or the operating system can be put into hardware to prevent tampering. Increasing the trustworthiness of the supporting software can also increase trust in the operating system. For instance, good network-security methods like encryption and well-tested communications protocols can prevent tampering with commands that cross the network, so their use encourages trust in the operating system.

TRANSACTIONS AND FEEDBACK WITH GOVERNMENT

Digital government should include more than making forms and reports accessible to citizens; it should permit citizens to affect government processes (Slayton & Arthur, 2003), to address Sztompka's factors of performance and precommitment. Citizens should be able to file applications for business permits online, for instance. Permitting such online transactions can simplify citizen's lives, reducing the amount of time they spend in government offices and waiting in lines, and may be the only possible way to deliver services for widely scattered governments and those of developing countries with limited infrastructures. Providing such services increases citizen trust that government procedures are functioning appropriately. Online transactions can also eliminate much of the opportunity for bribes and other forms of corruption, and can remove some of the subjectivity of bureaucratic decision-making by implementing some decisions with computer algorithms. This provides more fairness (Bovens & Stavros, 2002).

Digital government also permits feedback from citizens to the government to give citizens a better means to influence it. For instance, online surveys can assess citizen opinion, which is helpful even for nonrandom samples of citizens, or citizens can actually vote online. Proposed or existing laws and regulations can be subjected to comments on discussion boards, giving the government feedback about unanticipated problems, increasing the fairness of the laws and regulations and improving citizen trust in them.

MEASURING TRUST IN GOVERNMENT

It is valuable for a government to measure by surveys the degree of trust can that citizens have in it. (West, 2004) reports that digital government as currently implemented in the United States is not fostering much trust. (Welch & Hinnant, 2003) surveyed Americans to determine what features of electronic government were most supportive of trust by citizens. They discovered that both "transparency" (accessibility of government by information systems) and "interactivity" (ability of citizens to control government in some way) were correlated with trust in government; but frequent American users of digital government were less satisfied with the interactivity available than the transparency, which tended to decrease their total trust level. This suggests that interactivity must get more attention in future systems if they are to be well trusted by citizens.

FUTURE TRENDS

Digital government may be inevitable, but trust in digital government is another matter. Successful cultivation of trust by citizens is difficult for many governments today, and digital government is subject to many of the same stresses that make trust difficult. Clearly, good technical understanding, including human-engineering of the interface, is necessary to implement digital government successfully, and a successful implementation is one precondition of trust. But another factor is the degree to which citizen needs are met by the technology, and that requires perceptive political leadership. It is too early to say how the trust issue will be resolved in digital governments.

CONCLUSION

Digital government, like much technology, can either to improve government or make it worse. Digital government can provide advantages for the citizenry: Easier access to important information, more reliable implementation of procedures, and better accounting for actions including assignment of responsibility. If digital government is implemented well, these benefits should increase the trust of citizens in their government because they increase the appearance of trustworthiness, consistency of performance, and accountability for actions. But citizens are not very tolerant of incompetence in government, and digital government must be implemented with carefully designed and carefully tested technology to gain these benefits.

REFERENCES

Adam, N., & Worthmann, J. (1989, December). Security-control methods for statistical databases: a comparative study. *ACM Computing Surveys, 21* (4), 515-556.

Bovens, M., & Stavros, Z. (2002). From street-level to system-level bureaucracies: how information and communication technology is transforming administrative discretion and constitutional control. *Public Administration Review, 62* (2), 174-184.

Cronin, G. (1995, March). Marketability and social implications of interactive TV and the information superhighway. *IEEE Transactions on Professional Communication, 38* (1), 24-32.

Eckman, P. (2001). *Telling lies: clues to deceit in the marketplace, politics, and marriage*. New York: Norton.

Friedman, B., Kahn, P., & Howe, D. (2000, December). Trust online. *Communications of the ACM, 43* (12), 34-40.

Hardin, R. (2002). *Trust and trustworthiness*. New York: Russell Sage Foundation.

Josang, A. (2001, June). A logic for uncertain probabilities. *Intl. Journal of Uncertainty, Fuzziness, and Knowledge-Based Systems, 9* (3), 279-311.

Kofler, R., Krimmer, R., & Prosser, A. (2003, January). Electronic voting: algorithmic and implementation issues. *Proc. of 36th Hawaii Intl Conf. on System Sciences,* Honolulu, HI, 142a.

Levi, M., & Stocker, L. (2000). Political trust and trustworthiness. *Annual Review of Political Science, 3*, 475-508.

Mercuri, R. (2003, January). On auditing audit trails. *Communications of the ACM*, *46*(1), 17-20.

Nyberg, D. (1993). *The varnished truth: truth telling and deceiving in ordinary life*. Chicago: University of Chicago Press.

Postman, N. (1993). *Technopoly: the surrender of culture to technology*. New York: Vintage.

Prins, J. (Ed.) (2002). *E-government and its implications for administrative law: regulatory initiatives in France, Germany, Norway, and the United States*. London, UK: Cambridge.

Rowe, N. (2004, December). Designing good deceptions in defense of information systems. *Computer Security Applications Conference*, Tucson, AZ.

Slayton, R., & Arthur, J. (2003). Public administration for a democratic society: Instilling public trust through greater collaboration with citizens. In Malkia, M., Savolainen, R., & Anttiroiko, A.-V. (Eds.), *E-transformation in governance: new directions for government* (pp. 110-130). Hershey, PA: Idea Group.

Smith. R. (2001). *Authentication: from passwords to public keys.* Reading, MA: Addison-Wesley Professional.

Sztompka, P. (1999). *Trust*. Cambridge, UK: Cambridge University Press.

Theoharis, A. (Ed.) (1998). *A culture of secrecy: the government versus the people's right to know.* Lawrence, KS: University Press of Kansas.

Tolbert, C., & Mossberger, K. (2004). The effects of e-government on trust and confidence in government. Retrieved September 7, 2004 from www.digitalgovernment.org/dgrc/dgo2003/cdrom/PAPERS/ citsgovt/tolbert.pdf.

Wayner, P. (2002). *Disappearing cryptography: information hiding: steganography and watermarking.* San Francisco: Morgan Kaufmann.

Welch, E., & Hinnant, C. (2003, May). Internet use, transparency, and interactivity effects on trust in government. *Proc. of 36th Hawaii Intl Conf. on System Sciences,* Honolulu, HI, 144.

West, D. (2004, February). E-government and the transformation of service delivery and citizen attitudes. *Public Administration Review, 64* (15), 15-27.

Wilson, J. (2000). *Bureaucracy: what government agencies and why they do it.* New York: Basic Books.

Yu, H., Kundur, D., & Lin, C.-Y. (2001, July-September). Spies, thieves, and lies: the battle for multimedia in the digital era. *IEEE Multimedia, 8* (3), 8-12.

DEFINITIONS OF TERMS

access control: Limitations (usually automatic) on who can see or use something.

auditing: Keeping records of processes to later confirm they were performed properly.

authentication: Proving that someone is who they say they are; this is particularly important with online activities where one cannot see with whom one is interacting.

computer-illiterate: Lacking knowledge of how to use computers and software.

deception: Causing someone to infer a false idea; lying is one subcategory.

digital signature: Digital information attached to a digital document that proves who is responsible for it by use of a code known only to them.

secrecy: Prevention of access to information, enforced for digital data with encryption.
steganography: Embedding hidden messages in documents.
transparency, organizational: The ease by which the operations of an organization can be understood by outsiders.
trust: Confidence that future actions by others will fulfill our positive expectations, usually entailing reduced vigilance by us to monitor those actions and freed resources by us to do other things.