Chapter 12
Thinking Outside of the Ballot Box:
Examining Public Trust in E-Voting Technology

Susan K. Lippert
Drexel University, USA

Ekundayo B. Ojumu
IBM Global Services, USA

ABSTRACT

Electronic voting, or e-voting, is a relatively closed process that contains inherent risks associated with the potential for voting irregularities, translation errors, and inappropriate manipulation (Oravec, 2005). To develop a greater understanding of trust issues surrounding the use of e-voting, an investigation into the public trust and the relationship between trust and electronic voting technology were assessed. Men and women of various ethnicities, ages, educational backgrounds, technological experiences, political affiliations, and prior experience with e-voting participated in this study. Rogers’ (1995) taxonomy of adopters—innovators, early adopters, early majority, late majority, and laggards—was used to classify individuals based on their willingness to participate in e-voting. A principle-components factor analysis (PCFA) with separate tests for discriminant validity and multiple-regression analyses were used to confirm the hypotheses. The findings suggest that innovators and early adopters are more likely to trust technology and express an intention to use an e-voting system.
INTRODUCTION

Electronic voting, or e-voting, has been found to contain inherent risks for irregularities, errors, and inappropriate manipulation (Oravec, 2005). E-voting is the use of software and hardware to facilitate voting by individuals from either remote or poll-specific locations through a computer information system for casting votes. E-voting systems should ensure the privacy and authenticity of the voter, enable the individual to record only one vote, and remain secure from any unauthorized individuals tampering with the technology in an attempt to cast fraudulent votes.

The 2004 election in the United States encountered several problems with the e-voting process including technological issues when the New Orleans e-voting machines failed, resulting in frustrated voters and unwanted litigation (E-Voting Problems Reported as Election Gets Under Way, 2004). Additionally, an e-voting machine in Ohio added almost 4,000 votes for George W. Bush (Liptak, 2004) while in North Carolina, more than 4,500 votes were lost due to a storage problem (Computer Loses 4,500 Votes, 2004). These issues provide examples of technological and procedural anomalies associated with e-voting and underscore the need for protocols that ensure the verifiability of actual votes cast.

The United States is not alone in the use and development of e-voting. In fact, Ireland, Australia, the United Kingdom, and India have established independent commissions to investigate the use of e-voting technologies (Commission on Electronic Voting, 2005). The Government of Ireland established a commission on e-voting in March 2004 to evaluate a computer-aided voting and counting system proposed for use during the June 2004 elections. The commission indicated that it did not have a “requisite degree of confidence” in the chosen system based on issues of system testing, source-code reliability, accuracy of the software, and the security of the system. A key overriding factor cited in the report was the limited amount of time available to review the system prior to the proposed usage date.

Australian voters were first introduced to the Australian Capital Territory (ACT) e-voting system in the October 2001 election. This system was again used for parliamentary elections in October 2004 (ACT Legislative Assembly, 2001). This e-voting system uses personal computers as voting terminals and authenticates the votes with the use of a bar code. These voting terminals are connected to a secure server in each polling location. In the Australian model, individuals are not able to vote over public networks such as the Internet (ACT Legislative Assembly).

The Office of the Deputy Prime Minister in the United Kingdom is considering the use of e-voting for its next general election in 2008 (Implementing Electronic Voting in the UK, n.d.). While the UK government has yet to decide on a specific e-voting policy, it has a wide variety of possibilities under consideration including (a) enabling individuals to vote by telephone from home, (b) casting a ballot from a mobile phone, (c) using the Internet, or (d) recording choices through digital television configurations. Regardless of the specific application selected, there remain a number of issues of concern with the introduction of e-voting practices. These concerns include protecting privacy, maintaining security, enabling secrecy, and generating public confidence in e-voting systems (Implementing Electronic Voting in the UK, n.d.).

The Election Commission of India (2005) has considered the use of electronic voting machines (EVMs) as an alternative to traditional paper ballots used for electing candidates. The EVM contains a control unit and a balloting unit listing each candidate with a light adjacent to the button that the voter presses to indicate a selected candidate choice. Both components of the EVM operate through a battery power pack. The Election Commission suggests that the use of EVMs speeds the counting process, offers secrecy of voting data, and contains security features to ensure the integrity of recorded votes.