

9th Annual Privacy and Security Conference and Exposition

**Digital Dilemmas, Digital Dreams: Privacy,
Security and Society in New World
Networks**

February 7 - 8, 2008

Victoria, BC

PANEL C: ELECTRONIC VOTING: CAN ONE PERSON EQUAL ONE e-VOTE?

Friday February 8 , 2008, 2:05 – 3:10 PM

Richard S. Rosenberg, Professor Emeritus

Department of Computer Science

University of British Columbia

Vancouver, BC

President, BC Freedom of Information and Privacy Association

rosen@cs.ubc.ca

OUTLINE

- INTRODUCTION
- PRIVACY PROTECTION IN CANADA
- ELECTRONIC VOTING
- SOME PRIVACY ISSUES
- CONCLUSIONS

INTRODUCTION

- ❑ In the last few years, with the public's discovery of the Internet and the startling growth in use, electronic polling has become much more of a real possibility. Polls are a regular feature on the Internet, whether voting for Web-page layouts, songs, pinups-of-the-week, or presidential candidates.

Continued

- ❑ Of course, these polls are highly unscientific as there are no demographic controls, and they have little effect other than to provide marketing information, but there could potentially be a sufficient level of security in place to limit voting to registered voters. In this case, would it be used by governments, and if so, how and to what end?**

- Richard S. Rosenberg, *The Social Impact of Computers*, San Diego, CA: Elsevier Academic Press, 2004, p. 271.

Florida Elections of 2000

- But it was the difficulties in both voting and counting the votes in Florida as part of the year 2000 presidential election that led to the undertaking of many studies to evaluate the prospects of online voting, in the near future.**

An Early Study

- ❑ **One of the first such studies was carried out before the Florida election and reported early in 2001. It was sponsored by the National Science Foundation and was a joint effort of the Internet Policy Institute, the University of Maryland, and the Freedom Forum.**
- ❑ **Three possible applications of the Internet, namely, poll site Internet voting, kiosk voting, and remote Internet voting were proposed.**

Continued

- The first category is rather straight forward, bringing the convenience of the Internet to the traditional poll site, where since voting is still under the control of election officials, traditional security can be enforced.**
- The kiosk is a remote site, which could be located anywhere people congregate. It is possible for election officials to monitor and supervise the operation of these sites and security could involve television cameras as well.**

Remote Internet Voting

- ❑ Seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is Internet accessible.**
- ❑ While the concept of voting from home or work is attractive and offers significant benefits (e.g., the ability to conduct online research on candidates prior to voting, and the empowerment of the disabled), it also poses substantial security risks and other concerns relative to civic culture.**

Continued

- Without official control of the voting platform and physical environment, there are many possible ways for people to intervene to affect the voting process and the election results. Current and near-term technologies are inadequate to address these risks.**

Major Findings

- ❑ Poll site Internet voting systems offer some benefits and could be responsibly fielded within the next several election cycles.**
- ❑ Remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed.**
- ❑ Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented for the foreseeable future.**

2001 General Accountability Office Study

- ❑ **The broad application of Internet voting in general faces several formidable social and technological challenges. These include providing adequate ballot secrecy and privacy safeguards; providing adequate security measures to ensure safeguards against intentional intrusions and inadvertent errors; providing equal access to all voters, including persons with disabilities, and making the technology easy to use; and ensuring that the technology is a cost-beneficial alternative to existing voting methods.**

PRIVACY PROTECTION IN CANADA

□ Privacy as a Fundamental Right:

- Privacy, the Canadian Supreme Court has said, is at the heart of liberty in a modern state, and the limits the *Charter* imposes on government to pry into the lives of its citizens go to the essence of a democratic state.
- the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. (Justice Louis D. Brandeis, US Supreme Court, 1928)

Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)

□ Three Stages of Implementation:

- **Stage 1. As of January 1, 2001, the Act applied to every organization which operates as a federal work, undertaking or business.**
- **Stage 2. On January 1, 2002, the Act applied to personal health information.**
- **Stage 3. From January 1, 2004, the Act applied to every organization that collects, uses or discloses personal information in the course of commercial activity within a province.**

BC and Alberta Personal Information Privacy Acts

- ❑ **On October 12, 2004, the federal Cabinet exempted any organization to which BC's PIPA applies from application of the federal PIPEDA “in respect of the collection, use and disclosure of personal information that occurs in the Province of British Columbia.”**
- ❑ **BC PIPA took effect on November 10, 2004.**

Personal information

- ❑ **Personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:**
 - **name, age, weight, height**
 - **medical records**
 - **income, purchases and spending habits**
 - **race, ethnic origin and colour**
 - **blood type, DNA code, fingerprints**
 - **marital status and religion**
 - **education**
 - **home address and phone number**

The Law Gives You, the Individual, the Right to:

- **know why an organization collects, uses or discloses your personal information;***
- **expect an organization to collect, use or disclose your personal information reasonably and appropriately, and not use the information for any purpose other than that to which you have consented;***
- **know who in the organization is responsible for protecting your personal information;**

Rights Continued:

- **expect an organization to protect your personal information by taking appropriate security measures;**
- **expect the personal information an organization holds about you to be accurate, complete and up-to-date;**
- **obtain access to your personal information and ask for corrections;***
- **complain about how an organization handles your personal information.**

http://www.privcom.gc.ca/information/02_05_d_08_e.asp

The Law Requires Organizations to:

- **obtain your consent when they collect, use or disclose your personal information;***
- **supply you with a product or a service even if you refuse consent for the collection, use or disclosure of your personal information unless the information is essential to the transaction;***
- **collect information by fair and lawful means;**
- **have personal information policies that are clear, understandable and readily available.**
 - http://www.privcom.gc.ca/information/guide_e.asp

Exceptions

- ***There are exceptions to these principles. For example: an organization may not need to obtain your consent if collecting the information clearly benefits you and your consent cannot be obtained in a timely way; or if the information is needed by a law enforcement agency for an investigation, and getting consent might compromise the information's accuracy.**

ELECTRONIC VOTING

- ❑ **It is becoming clear that a realization of Internet voting is neither a given nor is it on the horizon. Many basic Internet security problems must be overcome as well as many specific voting security ones, as well as a number of social problems. In addition, there is much that can be done to improve the current system, short of implementing Internet voting prematurely.**

Caltech and MIT Voting Technology Project, 2001

- ❑ **The report notes that the number of lost votes [Between 4 and 6 million in the 2000 election] can be reduced by the adoption of the following measures:**
 - **Upgrade voting technologies. Replace punch cards and lever machines with optical scanners. We estimate 1.5 million of these lost votes can be recovered with this step.**
- Available at <http://www.netvoting.org/Resources/InternetVotingReport1.pdf>

Continued

- **Improve voter registration systems. We recommend improved database management, installing technological links to registration databases from polling places, and use of provisional ballots. We estimate this could save another 3 million lost votes. Aggressive use of provisional ballots alone might substantially reduce the number of votes lost due to registration problems.**

Future Recommendations

- We call for a new architecture for voting technology. This architecture will allow for greater security of electronic voting. It will allow for rapid improvement and deployment of user interfaces—that is, better ballots. It is a framework within which we can explode several myths about electronic voting.**

Continued

- ❑ There must be significant investment by the federal government in research and development of voting equipment technologies and meaningful human testing of machines.**
- ❑ The federal government should establish an independent agency to oversee testing and to collect and distribute information on the performance and cost of equipment.**

CONCLUSIONS

□ **Rebecca Mercuri:**

- **These problems [in some currently available systems] result from an underlying fundamental conflict in the construction of electronic voting (e-voting) systems: the simultaneous need for privacy and auditability, which is the ability, when necessary, to recount the votes cast. Privacy is critical to a fair election, necessary to prevent voter coercion, intimidation, and ballot-selling.**

- **“A Better Ballot Box,” IEEE Spectrum Online, Oct. 2002.**

Continued

- **But maintaining the voter's privacy precludes the use by computer-based products of standard audit and control practices: logging transactions and identifying them from end to end. In other words, the privacy constraint directly conflicts with the ability to audit the ballot data.**

Continued

- **For the system to work, there must be a way to backtrack vote totals from actual ballots that come from (and must be independently verified by) legitimate voters voting no more than once. In turn, the ballot must in no way identify or be traced back to the voter after it is cast. These constraints, many experts say, cannot be mutually satisfied by any fully automated system.**

Hacking the Vote*

□ **Reliability, more than fraud, bugs voting machines:**

➤ **The problem with direct-recording-electronic (DRE) voting systems like Diebold's Accuvote and others from Election Systems and Software (ES&S) and Hart InterCivic is their vulnerability to sloppy installation, poor maintenance, shoddy software, infrequent updates and accidental loss of data.**

• **The Economist, Jan. 25, 2008**

Continued

- **A team of computer scientists—three from Johns Hopkins University and one from Rice University—subsequently published a scholarly critique of the Diebold software. They found hundreds of flaws in the source code, ranging from lack of password protection on the main database to bugs that allowed people with a certain type of smart-card to vote as many times as they liked. The software provided no way to verify that a vote had been correctly recorded, and no permanent record was kept. The company claimed that particular software was out of date, and had never actually been used in an election.**

Continued

- **On all machines, the root cause of the poor security was the way standard practices for key and password management, security hardware and cryptography had been blindly ignored. Auditing was virtually non-existent. Logs of events happening during an election could be easily forged or erased by those operating the system. In all cases, the software was deemed “fragile” at best.**

Why Push Electronic Voting Machines? Follow the Money Trail

- ❑ **Expert studies have shown that the quality of all commercially available e-voting systems is abysmal, and that they are vulnerable to large-scale fraud.**
- ❑ **Touch-screen machines are particularly bad because there are no independent records of cast ballots. So, if reported results are challenged, meaningful recounts are impossible.**
 - [Stephen J. Unger, January 27, 2008](#)
 - www.lohud.com/apps/pbcs.dll/article?AID=/20080127/OPINION/801270311/1076/OPINION03

Finally

- ❑ **In Canada, in most other industrialized countries, in most Maine precincts, and in parts of several other states, hand-marked ballots are hand-counted. This process is simple, robust, transparent to all, and, assuming Boss Tweed is not in charge, not vulnerable to large-scale fraud. Simple systems exist to help handicapped people generate paper ballots countable along with mainstream ballots.**