

Report of the National Workshop on Internet Voting: Issues and Research Agenda

March 2001



Sponsored by the National Science Foundation

**Conducted in cooperation with the University
of Maryland and hosted by the Freedom Forum**

The Internet Policy Institute

The Internet Policy Institute (IPI) is the nation's first independent, nonprofit research and educational institute created exclusively to provide objective, high-quality analysis and outreach on economic, social and policy issues affecting and affected by the global development and use of the Internet. IPI is nonpartisan and does not lobby or otherwise actively advocate or represent the interests of businesses, associations, policy makers or others. A primary role for the Institute is as a forum for independent research, discussion, debate, and consensus building.

<http://www.internetpolicy.org>

The University of Maryland, College Park

The University of Maryland, College Park is a public research university, the flagship campus of the University System of Maryland, and the original 1862 land grant institution in Maryland. The University of Maryland is committed to achieving excellence as the state's primary center for research and graduate education and as the institution of choice for undergraduate students of exceptional ability.

<http://www.umd.edu>

The Freedom Forum

The Freedom Forum, based in Arlington, Va., is a nonpartisan, international foundation dedicated to free press, free speech and free spirit for all people. The foundation focuses on four main priorities: the Newseum, First Amendment issues, newsroom diversity and world press freedom.

<http://www.freedomforum.org>

The National Science Foundation

The National Science Foundation (NSF) is an independent federal agency that supports fundamental research and education across all fields of science and engineering, with an annual budget of nearly \$4.5 billion. NSF funds reach all 50 states, through grants to about 1,600 universities and institutions nationwide. Each year, NSF receives about 30,000 competitive requests for funding, and makes about 10,000 new funding awards.

<http://www.nsf.gov>

The Internet Policy Institute presents this publication as a useful contribution to public discourse. The findings, interpretations and conclusions in this publication are those of the authors and do not necessarily represent the views of the staff of the Internet Policy Institute or its Board of Directors.

© 2001 Internet Policy Institute

Preface

As use of the Internet in commerce, education and personal communication has become common, the question of Internet voting in local and national elections naturally arises. In addition to adding convenience and precision, some believe that Internet voting may reverse the historical and downward trend of voter turnout in the United States. For these reasons President Clinton issued a memorandum in December 1999 requesting that the National Science Foundation examine the feasibility of online (Internet) voting.

As a consequence, the Internet Policy Institute along with the University of Maryland conducted an NSF-sponsored workshop on October 11 and 12, 2000. Held less than a month before the national election, the workshop set out to examine the feasibility of Internet voting and to recommend a research agenda as needed to facilitate Internet voting. Thirty-five invitees participated; they spanned a range of voting expertise including state election officials, social scientists from academe, Internet security specialists and experts in voter fraud. Most had already been active in electronic and Internet voting studies and some had examined Internet or electronic elections at local and state levels. As the technological and social science issues were debated over the course of the workshop, it became apparent to all that ensuring the integrity of elections while preserving public confidence in the election process becomes increasingly complex when voting is moved to the Internet. Basically, it's a lot harder than it looks at first.

Many of the challenges to Internet voting do not lend themselves to easy solutions and this is especially true for voting from remote locations like your home or office. These challenges must be resolved prior to wholesale changes to the nation's election processes. The knowledge base for addressing the shortcomings of election systems is not large and hence there is an urgent need for focused research in the near and longer terms.

The contested 2000 Presidential election highlighted awareness of the critical importance of ensuring confidence in the integrity and fairness of election systems. As policy makers and election officials debate improvements in the months ahead, we believe the findings and recommendations for research contained herein offer timely and constructive wisdom that can light the pathway to our electoral future.



C.D. Mote, Jr.

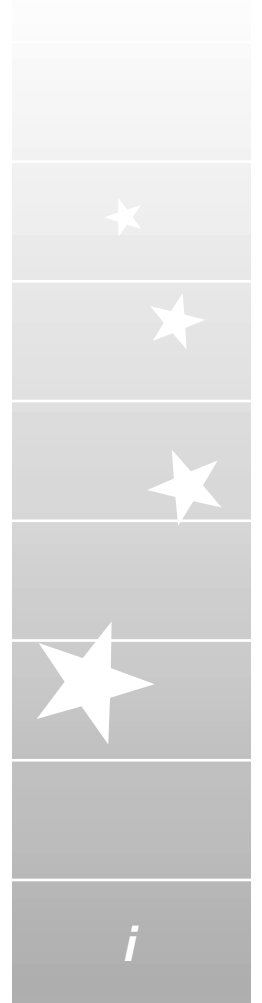


Table of Contents

Preface.....	i
Panelists	iii
Executive Summary	1
1. Introduction	5
1.1 The Interest in Online Voting	5
1.2 Project Overview	5
1.3 Definitions	6
2. The Evolution of Voting Systems.....	9
2.1 Conventional Systems	9
2.2 Voting Processes	9
2.3 Internet Voting Systems	10
2.4 Criteria for Election Systems	11
3. Technology Issues	13
3.1 Voting System Vulnerabilities	13
3.2 Reliability	17
3.3 Testing, Certification, and Standards	18
3.4 Specifications and Source Code	20
3.5 Platform Compatibility	21
3.6 Secrecy and Non-Coercibility	22
3.7 Comparative Risk	23
4. Social Science Issues	24
4.1 Voter Participation.....	24
4.2 Voter Access	25
4.3 The Election Process.....	26
4.4 Voter Information	28
4.5 Deliberative Democracy	28
4.6 Community and the Character of American Elections	29
4.7 Federal, State, and Local Roles	30
4.8 Legal Concerns	31
4.9 Voter Registration	33
5. Findings and Recommendations	34
5.1 Feasibility of Internet Voting	34
5.2 Research Issues	35
5.3 Research Methods	39
Appendices	
A. White House Memorandum	41
B. Workshop Registered Attendees	43
C. Glossary	45
D. Selected References	47
Acknowledgments	50
IPI Board of Directors	51
IPI Research Advisory Board	52

Panelists

Executive Committee

C.D. Mote, Jr., University of Maryland (Chairman)
Erich Bloch, Washington Advisory Group
Lorrie Faith Cranor, AT&T Research Labs
Jane Fountain, Harvard University
Paul Herrnson, University of Maryland
David Jefferson, Compaq Systems Research Center
Thomas Mann, The Brookings Institution
Raymond Miller, University of Maryland
Adam C. Powell, III, The Freedom Forum
Frederic Solop, Northern Arizona University

Panelists

Michael Alvarez, California Institute of Technology
Penelope Bonsall, U.S. Federal Election Commission
David Brady, Stanford University
Polli Brunelli, U.S. Federal Voter Assistance Project
Paul Craft, Division of Elections, Florida Department of State
Craig Donsanto, U.S. Department of Justice
David Elliot, Elections Division, Washington Department of State
Michael Fischer, Yale University
Dan Geer, @Stake, Inc.
Lance Hoffman, George Washington University
Patricia Hollarn, Supervisor of Elections, Okaloosa County, Florida
Carl Landwehr, Mitretek Systems, Inc.
Richard Niemi, University of Rochester
Ronald Rivest, Massachusetts Institute of Technology
Aviel Rubin, AT&T Research Labs
Roy Saltman, Consultant
Barbara Simons, Association for Computing Machinery
Sandra Steinbach, Elections Division, Iowa Department of State
Mike Traugott, University of Michigan
Raymond Wolfinger, University of California, Berkeley

National Science Foundation Sponsors

Lawrence Brandt, Project Officer, Digital Government Program
Valerie Gregg, Digital Government Program
Frank Scioli, Political Science

Internet Policy Institute Project Staff

David W. Cheney, Principal Investigator
Richard M. Schum, Project Director

Executive Summary

Introduction

Elections are one of the most critical functions of democracy. Not only do they provide for the orderly transfer of power, but they also cement citizens' trust and confidence in government when they operate as expected. Although election systems are normally the province of election officials, the events that transpired in Florida during the 2000 presidential election focused national attention on how elections are administered. The subject of voting systems has taken center stage, and is under intense scrutiny by policymakers, interest groups, and the American people in general.

Over the last year, there has been strong interest in voting over the Internet as a way to make voting more convenient and, it is hoped, to increase participation in elections. Internet voting is seen as a logical extension of Internet applications in commerce and government. In the wake of the 2000 election, Internet systems are among those being considered to replace older, less reliable systems. Election systems, however, must meet standards with regard to security, secrecy, equity, and many other criteria, making Internet voting much more challenging than most electronic commerce or electronic government applications.

This report addresses the feasibility of different forms of Internet voting from both the technical and social science perspectives, and defines a research agenda to pursue if Internet voting is to be viable in the future. It is based on a workshop that took place before the 2000 election, but it nonetheless addresses many of the issues that are now being debated about what to do to improve the integrity of elections. The topics addressed here, while all related to Internet voting, are also relevant to discussions about other electronic voting systems.

Internet Voting by Type

Internet voting systems can be grouped into three general categories: poll site, kiosk, and remote. Each of these categories define the location where the ballot is cast, which, in turn, defines the social science and technical hurdles that are associated with each type of system. *Poll site Internet voting* offers the promise of greater convenience and efficiency than traditional voting systems in that voters could eventually cast their ballots from many polling places, and the tallying process would be both fast and certain. Since election officials would control both the voting platform and the physical environment, managing the security risks of such systems is feasible.

In *kiosk voting*, voting machines would be located away from traditional polling places, in such convenient locations as malls, libraries, or schools. The voting platforms would still be under the control of election officials, and the physical environment could be modified as needed and monitored (e.g., by election officials, volunteers, or even cameras) to address security and privacy concerns, and prevent coercion or other forms of intervention. Kiosk voting terminals pose more challenges than poll site systems, but most of the challenges could, at least in principle, be resolved through extensions of current technology.

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. 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.

Findings on Feasibility

Poll site Internet voting systems offer some benefits and could be responsibly fielded within the next several election cycles. While many issues remain to be addressed, the problems associated with these systems appear likely to be resolvable in the near term. As such, it is appropriate for experiments to be conducted and prototypes deployed in order to gain valuable experience prior to full-scale implementation. This would provide a basis for evaluating poll site voting compared to other voting systems. If found to be preferable to other systems, poll site Internet voting could be deployed in several phases. For instance, voters might first cast their ballots at the precinct level, then from anywhere within the county, and finally from anywhere within the state. The latter step would require registration and voter systems in the different counties to work together.

The next step beyond poll site voting would be to deploy kiosk voting terminals in public places. This path toward greater convenience would enable technologists and social scientists to address the many issues that confront the voting process at each level of implementation. Many issues related to kiosk voting, such as setting standards for electronically authenticating voters, still need to be resolved.

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. The security risks associated with these systems are both numerous and pervasive, and, in many cases, cannot be resolved using even today's most sophisticated technology. In addition, many of the social science concerns regarding the effects of remote voting on the electoral process would need to be addressed before any such system could be responsibly deployed.¹ For this reason, it is imperative that public officials educate themselves about the dangers posed by remote Internet voting, and the ramifications of failure on the legitimacy of the electoral process.

Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented until an adequate authentication infrastructure is available and adopted. While information already in the domain of election officials may be updated remotely, given appropriate authentication protocols, initial registration conducted online cannot establish the identity of the registrant without the transmission of unique biometric (fingerprint or retinal scan) data and an existing database with which to verify the data. Online registration without the appropriate security infrastructure would be at high risk for automated fraud (i.e., the potential undetected registration of large numbers of fraudulent voters). The voter registration process is already one of the weakest

¹ However, remote Internet voting may be appropriate in the near-term for special populations, such as the military and government employees and their dependents based overseas. Such exceptions should be evaluated on a case-by-case basis.

links in our electoral process. The introduction of Internet-based registration without first addressing the considerable flaws in our current system would only serve to greatly exacerbate the risks to which we are already exposed.

Research Recommendations

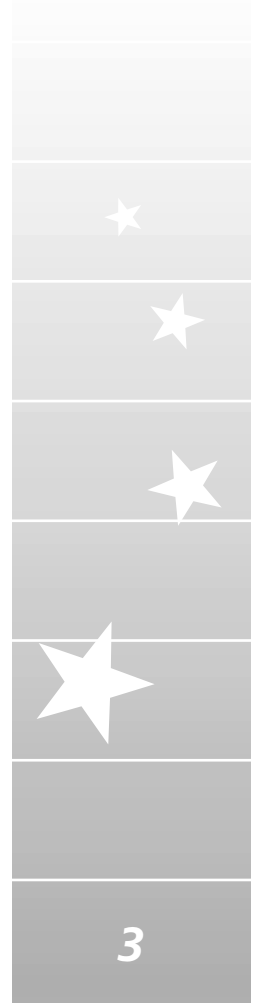
One important result of the 2000 presidential election is that it has brought about a rare opportunity for reform in election systems and administration. Many jurisdictions around the nation are currently facing once-in-a-generation decisions on which type of system to procure and how to improve their procedures. It is critical that election officials make informed decisions based on a solid and current body of knowledge.

In addition, there is likely to be substantial public and political pressures to adopt remote Internet voting in the near future, despite the serious concerns of election officials, social scientists, and security and other information technology experts. It is vital, therefore, that research efforts begin immediately so that policymakers will have the requisite information to make responsible decisions regarding the deployment of Internet voting systems.

Research is required to address issues related to poll site, kiosk, and remote Internet voting. The needed research includes a mix of short- and long-term research, and covers technical, social science, and election systems topics. Most research topics encompass several of these categories. Critical research areas include:

- Approaches to meeting the security, secrecy, scalability, and convenience requirements of elections.² Particular emphasis should be placed on the development of secure voting platforms, and secure network architectures (Section 5.2.1);
- Development of methods to reduce the risk of insider fraud (Section 5.2.1);
- Development of reliable poll site and kiosk Internet voting systems that are not vulnerable to any single point of failure and cannot lose votes (Section 5.2.2);
- Development of new procedures for continuous testing and certification of election systems, as well as test methods for election systems (Section 5.2.3);
- The effects of potential open architecture and open source code requirements on innovation, profitability, and public confidence (Section 5.2.3);
- Human factors design for electronic voting, including the development of appropriate guidelines for the design of human interfaces and electronic ballots, as well as approaches to addressing the needs of the disabled (Section 5.2.4);
- Protocols for preventing vote selling and reducing coercion (Section 5.2.5);
- The economics of voting systems, including comparative analyses of alternative voting systems (Section 5.2.6);
- The effects of Internet voting on participation in elections, both in general and with regard to various demographic groups—especially those with less access to or facility with computers (Section 5.2.7);
- The effects of Internet voting on elections, the public's confidence in the electoral process, and on deliberative and representative democracy (Section 5.2.8);
- The implications of Internet voting for political campaigns (Section 5.2.9);

² In many cases, research is needed at both the level of component technologies and at the level of election systems.



- The appropriate role of the federal government in state-administered elections (Section 5.2.10);
- Legal issues associated with and the applicability of existing statutes to Internet voting, including jurisdiction, vote fraud, liability for system failures, international law enforcement, and electioneering (Section 5.2.11);
- Electronic authentication for kiosk and remote voting (Section 5.2.12); and
- Experimentation, modeling, and simulation of election systems (Section 5.3.3).

Because most issues related to Internet voting require a balance between security, convenience, and cost, it is critical that this research be conducted in an interdisciplinary manner. And, since any remedy must meet the practical needs of election administration, these research efforts should involve election officials from their inception. Social scientists, information technologists, and election officials need to collaborate to address questions that are essential to the future of our democratic system.

In many of these research areas, there is a need for both nearer-term analyses and longer-term fundamental research and technology development. For nearer-term analyses, the present level of funding and the pace of activity are too low to address the issues surrounding new voting technologies in a timely manner. The workshop, however, did not address the issue of who should do the nearer-term analyses. The Federal Election Commission, the individual states, the National Association of State Election Directors (NASSED), and the National Institute of Standards and Technology (NIST), as well as other organizations, have done work in the past related to the analysis of election issues, standards, test methods, and certification processes.

With regard to longer-term research issues, it is highly appropriate for the National Science Foundation (NSF) to support a spectrum of research in technical and social science fields, and to conduct advanced technology pilot projects involving multidisciplinary research teams, government agencies, and/or election officials in meaningful collaboration. It is also appropriate for the NSF to support forums, workshops, and information exchanges that bring together election officials, government agencies, the private sector, and academia to address issues related to the unique challenges of Internet voting systems.

The research topics outlined in this report are drawn from the large, diverse, intellectually challenging, and important research agenda related to Internet voting. Internet voting promises significant benefits to democratic processes, but also poses great challenges. The pursuit of this agenda is essential to address these challenges, and to make sound decisions about the future of election systems in America.

1. Introduction

1.1 The Interest in Internet Voting

The explosion of the Internet culture in the United States and elsewhere has caused many to question why we should not be able to cast our ballots in the same manner as we order books on the Web—from home or from work. Voters see themselves as customers and expect government to make the business of voting more convenient. Recent efforts by government toward using the Internet to provide services and information have fueled this argument, as have the active efforts of vendors of Internet voting systems. Indeed, the concept of “digital democracy” has attracted many followers.

Most proponents of Internet voting argue that the adoption of such systems would increase voter participation, especially among youths, overseas personnel, business and holiday travelers, and institutionalized or house-bound voters. Increasing voter participation is especially of interest because voter turnout has been low and declining in the United States. Some people also suggest that Internet voting would, in the long run, reduce the costs of elections. These claims, however, remain largely untested. And while enhancing convenience and access is a worthy goal, there are other considerations, such as security, ballot secrecy, privacy, cost, and equality of access to voting. In many cases, there are trade-offs among these considerations and election officials must determine how best to strike a responsible balance.

Due to the increasing reliance on the Internet to communicate with others, conduct business, and access government services, some people believe that the move to Internet voting is all but inevitable—the public will demand it and the politicians will respond. If so, the question is whether election officials—and the broader policy community—will be able to resolve the many issues that confront Internet voting in order to make sound decisions that preserve and enhance the quality of the electoral process.

1.2 Project Overview

As part of efforts to make government services more accessible through use of the Internet, the President directed the National Science Foundation (NSF) to conduct a one-year study to examine the feasibility of online voting (see Appendix A). Pursuant to this directive, the NSF awarded a grant to the Internet Policy Institute (IPI) to conduct a workshop to examine the issues associated with conducting public elections over the Internet, and to identify areas for future research.

Held on October 11 and 12, 2000, the workshop brought together a diverse group of distinguished computer and social scientists, election officials, and other specialists in an effort to find consensus on these topics. The sessions were open to the public and Web cast live, courtesy of the Freedom Forum. A very knowledgeable group of observers from many sectors participated in—and contributed to—the discussions (see Appendix B).

The workshop covered a broad range of issues from diverse points of views. These issues included the evolution of voting systems, the criteria that election systems should satisfy, a wide variety of technical and social science concerns, and the practical problems that election officials face in certifying and implementing complex systems.

At the time of the workshop, it was widely believed that the prime public interests in Internet voting were in increasing convenience and in increasing participation in elections. Consequently, the main interest was in remote Internet voting—the casting of votes from any computer connected to the Internet. There was relatively little focus on poll site Internet voting. It was generally assumed that current election systems had acceptable levels of security, accuracy, and reliability.

The 2000 presidential election, and the subsequent five-week period in which the election results were in doubt, changed the context of the online voting debate. There is now widespread interest in improving the accuracy and reliability of election systems, and increased convenience has become a secondary concern. As a result, this report has, in some cases, gone beyond the discussion at the workshop, especially with regard to an increased focus on issues related to poll site Internet voting.

This report is intended to perform two different functions for two different audiences. First, it provides an assessment of the current feasibility of Internet voting. The main audiences for this purpose are the public officials and broader policy community who must make decisions on election systems. The second function is to identify the key research priorities with regard to Internet voting. The main audiences for this purpose are the research community, the NSF, and other entities involved in supporting research.

Although the report largely reflects the information provided and views expressed at the workshop, in some cases it goes a bit further, both in the detail that it provides and in its recommendations. The recommendations are those of the executive committee of the project, which used its own expertise and judgment to synthesize, prioritize, and augment the findings of the workshop.

The report begins with some key distinctions between different types of online voting and elections. It provides some background on current voting systems, and describes the criteria that elections systems are expected to meet. Next, it addresses a wide range of technical and social science issues that were the main focus of the workshop. It concludes with findings regarding the feasibility of each type of Internet voting and recommendations for research.

1.3 Definitions

The term “Internet voting” encompasses a variety of concepts. Principally, it can be distinguished both by the nature of the election (public or private) and the voting site (poll site, kiosk, or remote).

1.3.1 *Internet Voting by Type*

Poll site Internet voting refers to the casting of ballots at public sites where election officials control the voting platform (i.e., the hardware and software used to vote and the physical environment of the voting place). In these kinds of systems, clients are intended to be accessed only at the poll site under the observation of election officials. *Remote Internet voting* refers to the casting of ballots at private sites (e.g., home, school, office) where the voter or a third party controls the voting client. Ideally, this type of open network system would enable voting from virtually anywhere at anytime; however, as discussed later in this report, the concomitant risks are significant.

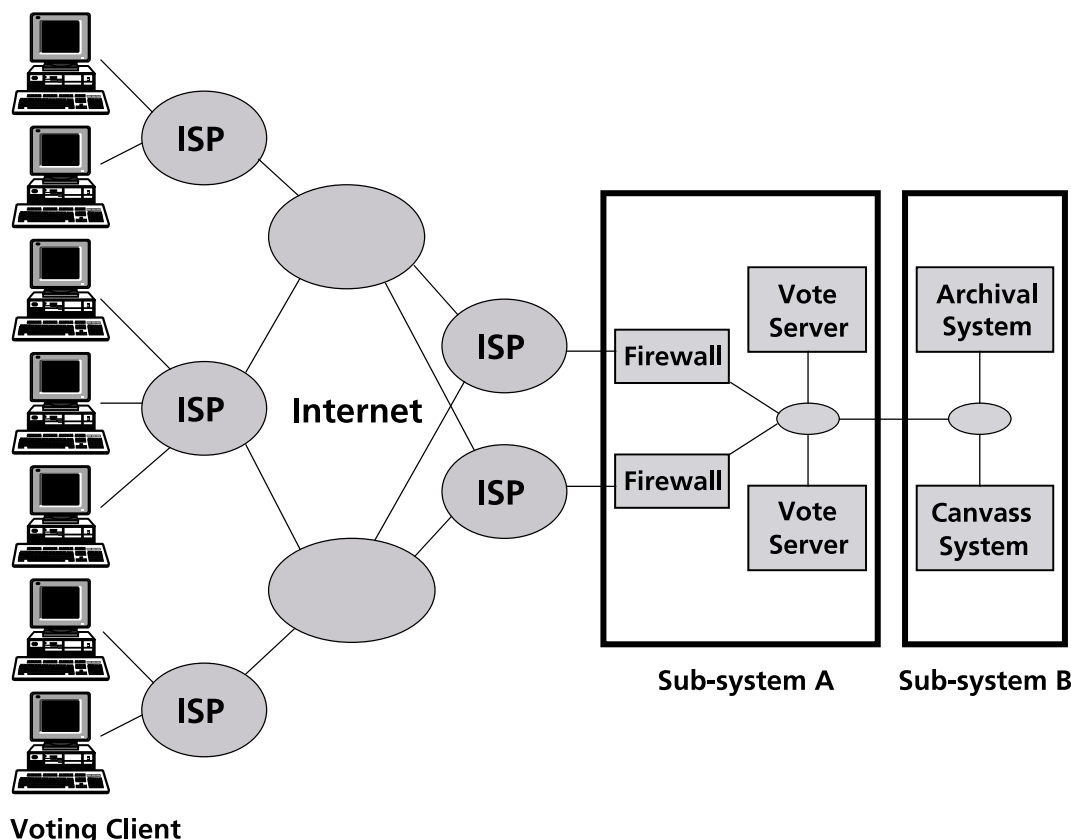


Figure 1: A schematic sketch of a generic Internet voting system. In poll site voting, the voting clients would be precinct voting terminals, whereas in remote voting, these would be individual computers in homes and workplaces. The clients are connected to one or more Internet service providers (ISPs), and to the ISPs at the server side of the system through the Internet. The server side is divided into two parts: sub-system A, that collects encrypted votes; and sub-system B, that decrypts ballots, tallies and archives votes, and produces reports.

While remote Internet voting has attracted the most public and media attention, and is often considered synonymous with Internet voting, there are many issues—both technical and policy-related—that must be resolved before remote voting is feasible. As discussed below, poll site voting, is much more viable in the near-term.

Another option, commonly referred to as *kiosk voting*, offers an intermediate step between poll site and remote voting. In this model, voting terminals would be tamper-resistant and located in convenient places like malls, post offices, or schools, but remain under the control of election officials. Kiosk voting could be monitored by election officials, observers, or even cameras to address security and privacy concerns, and prevent coercion or other forms of intervention. The challenges and risks associated with kiosk voting are considerable, but more approachable than those associated with remote voting.

It is also important to distinguish between the various kinds of Internet voting and other forms of electronic voting, usually referred to as direct recording electronic (DRE) voting. In DRE voting, the balloting process is performed on an electronic voting machine that records and stores the votes internally. It is possible, however, to have these DRE machines send their counts electronically to a central site (through either a direct dial-up

connection or a dedicated line). This would perform much the same function as a poll site Internet voting system, but without connecting to the Internet.

1.3.1 Public vs. Private Elections

Public elections are conducted under the jurisdiction of state election officials and are subject to federal and state election laws. Public elections must meet standards and legal tests that are generally more rigid and rigorous than for private elections.

There are several key differences between public and private elections. Fundamentally, the legitimacy of democratic institutions depends upon the extent to which the will of the people is represented. Because public elections are the vehicles by which that will is determined, the integrity of the election process is a matter of the highest national interest. As such, public elections tend to attract greater attention and face a higher likelihood of fraud and attack.

Equality of access is an essential goal for public elections. Similarly, voter privacy and ballot secrecy has been a requirement for public elections since the adoption of the Australian ballot at the turn of the 20th century.³ Moreover, the logistical and procedural considerations of administering elections are frequently more complex than for private elections. Ballots must accommodate many candidates and propositions, and are unique to each jurisdiction. Often, multiple languages and a write-in capability need to be supported.

While private elections may meet many of these same criteria, they often do not need to meet all of them. For example, many private elections do not require privacy and allow for voting by proxy. Over the past few years, private elections conducted over the Internet have become increasingly common. Many corporations now allow their shareholders to vote online, and a variety of organizations, including unions, colleges, and professional societies, are looking to Internet voting to save time and expense. For example, the Internet Corporation for Names and Numbers (ICANN) recently conducted a global election for executive board members online.

Other elections are essentially hybrids between public and private elections. Two of the most publicized uses of Internet voting systems to date, the 2000 Arizona Democratic Party and the Reform Party presidential primaries, were not run by state election officials, but were still subject to some aspects of state and federal election law.

The growth in online private elections is likely to spur greater interest in and demand for online public elections in the years ahead. Private elections are also likely to stimulate advances in technology, and provide experience in Internet voting that will be useful to public elections. Not all of that experience, however, can be applied directly to the different circumstances of public elections.

This report focuses largely on public elections, and the reader should assume that the issues addressed below pertain to public elections, except where noted.

³ The concept of an official, government-printed ballot that listed all the candidates was first introduced in the United States by Massachusetts in 1888, borrowing from the Australian practice.

2. The Evolution of Voting Systems

2.1 Conventional Voting Systems

In the United States, national elections are, in fact, many state-wide elections conducted independently by local election jurisdictions. Oregon, for example, has 36 election officials while Michigan has over 7000. Most states use a variety of different voting systems, with the actual procurement decisions being made by each county. These include:

Paper ballots: Voters mark boxes next to the names of candidates or issue choices, and place them in a ballot box. The ballots are counted manually. Paper ballots are also widely used for absentee ballots. Their drawback is that counting is laborious and subject to human error.

Mechanical lever machines: Voters cast ballots by pulling down levers that correspond to each candidate or issue choice. Each lever has a mechanical counter that records the number of votes for that position.

Punch cards: Voters punch holes in computer-readable ballot cards. Some systems use mechanical hole-punch devices for punching the holes while others provide the voter with pins to punch out the holes. The latter have been more subject to incomplete punches, resulting in more errors in reading the cards.

Optical scan devices: Voters record choices by filling in a rectangle, circle, or oval on the ballot. The ballots are read by running them through a computer scanner, which then records the vote.

Direct Recording Electronic (DRE) devices: Special-purpose or PC-based computers are used as voting machines. Voters use touch screens or push buttons to select choices, which are stored electronically in the memory of the machine. There are no paper ballots, and no paper record independent of the electronic memory.

2.2 Voting Processes

In addition, a variety of voting processes are employed throughout the nation. The most common is traditional voting at the poll site on Election Day. However, there are several alternative methods, including:

Absentee ballots: All states provide for the use of absentee ballots, which allow people to vote-by-mail before the election. Some states provide absentee ballots only to those people who certify that they are unable to get to the polling place on Election Day, for such reasons as travel or disability. Other states, such as Washington, provide absentee ballots to any registered voter who requests one.

Vote-by-mail: Oregon is the first, and so far only, state to adopt all mail voting.⁴ Oregon mails ballots to all registered voters, who generally return the filled-in ballots by mail. There are no longer any traditional polling places, although each county provides booths where people can fill out their ballots in privacy and places where they can directly deposit their ballots. Most election jurisdictions have not adopted vote-by-mail and restrict the use

⁴ The state adopted this form of balloting beginning with the 2000 presidential primaries and election.



of absentee ballots, in part because of security concerns. With absentee ballots, a person can be observed filling out the ballot, and there is a greater possibility for a person to sell their vote or to be subject to coercion. There is also no timely feedback to indicate whether a mailed ballot has been received by election officials in time to be counted.

Satellite voting: Many voting jurisdictions in the country allow early voting from satellite sites around a county for period of time (several weeks to a few days) prior to elections. In Texas, for example, mobile voting vans are used to bring voting to convenient locations.

Most of these alternatives to traditional poll site voting have been put forth in recent years in order to increase access, convenience, and turnout, and to make the voting population, which is inherently self-selective because voting is voluntary, look more like the citizenry at large. In general, however, these reforms have had little effect on turnout or on making under-represented groups vote in greater numbers. Changes in voting procedures have also frequently been made in the context of short-term political goals, such as to increase participation or support from a particular demographic group.

The long-term consequences of voting reforms have often differed from the initial expectations. Politicians and elites (e.g., political consultants, interest groups, opinion leaders) adapt to the reform, and then there is further adaptation by the electorate. Innovations usually benefit one party initially, and then the other party catches up. The end result is often different from the original intent. For example, when poll watchers from each party were added to the election process, they were originally intended to question the qualification of voters. But the parties now use them to figure out who has not yet voted and what groups need to be mobilized. Each change in election procedures leads to changes by political campaigns. In states where voting by mail takes place over an extended period before Election Day, the political campaigns have adapted by making get-out-the-vote drives last the entire voting period.

States also have varying voter registration requirements. All of the states, except North Dakota, require voters to register before voting. Most states require voters to register in advance, while a few, such as Wisconsin, allow registration on the day of the election.

2.3 Internet Voting Systems

Against this backdrop of diverse and decentralized election systems and processes comes interest and experimentation with Internet voting. As of the date of the workshop, there had been no widespread use of Internet voting in public elections. There had been, however, several well-publicized uses of Internet voting, including the 2000 Arizona Democratic presidential primary, the 2000 Reform Party primary, and a global election for ICANN, as well as several smaller-scale public experiments and numerous private elections.

Four counties in California and one in Arizona conducted mock election trials for the November 7, 2000 election. The Federal Voter Assistance Project (FVAP), a project of the Department of Defense, conducted a small-scale pilot project of remote Internet registration and voting for fewer than 100 absentee military and overseas voters from selected jurisdictions. Participants in the workshop also mentioned experiments in other countries, including Croatia and Costa Rica.

2.4 Criteria for Election Systems

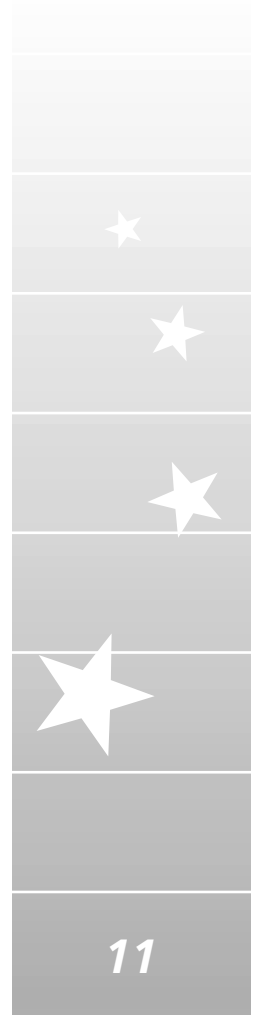
Based on the tradition of elections and voting systems in the United States, elections systems—whether through traditional voting methods or Internet voting—are commonly expected to satisfy a number of criteria, including:⁵

- *Eligibility and Authentication*—only authorized voters should be able to vote;
- *Uniqueness*—no voter should be able to vote more than one time;
- *Accuracy*—election systems should record the votes correctly;
- *Integrity*—votes should not be able to be modified, forged, or deleted without detection;
- *Verifiability and Auditability*—it should be possible to verify that all votes have been correctly accounted for in the final election tally, and there should be reliable and demonstrably authentic election records;
- *Reliability*—election systems should work robustly, without loss of any votes, even in the face of numerous failures, including failures of voting machines and total loss of Internet communication;
- *Secrecy and Non-Coercibility*—no one should be able to determine how any individual voted, and voters should not be able to prove how they voted (which would facilitate vote selling or coercion);
- *Flexibility*—election equipment should allow for a variety of ballot question formats (e.g., write-in candidates, survey questions, multiple languages); be compatible with a variety of standard platforms and technologies; and be accessible to people with disabilities;
- *Convenience*—voters should be able to cast votes quickly with minimal equipment or skills;
- *Certifiability*—election systems should be testable so that election officials have confidence that they meet the necessary criteria;
- *Transparency*—voters should be able to possess a general knowledge and understanding of the voting process; and
- *Cost-effectiveness*. election systems should be affordable and efficient.

For new election systems to be adopted, it is likely that they will need to satisfy all, or nearly all, of these requirements. In addition, it is important to consider how new election systems affect other aspects of American democracy, such as:

- Voter registration;
- Participation and access by demographic groups;
- Election logistics, administration, and costs;
- The nature of deliberative and representative democracy;
- The sense of community and character of America elections;
- The concept of federalism, and the appropriate roles of federal, state, and local government; and
- Election laws.

⁵ The workshop panelists identified the following list as criteria that must be addressed by any successful election system.



While each of these topics can be discussed separately, there is substantial interaction and many trade-offs among them. For example, efforts to improve security generally increase costs, reduce convenience and flexibility, and complicate implementation. The following sections address these topics individually, but also attempt to identify the areas where they overlap.

The discussion starts with the more technical topics and proceeds to the social science issues because many of the technical issues need to be addressed before the social science issues become significant. In particular, most of the social science effects of Internet voting pertain primarily to remote Internet voting, which, as the discussion of the technical issues makes apparent, should not be considered an immediate option.

3. Technology Issues

3.1 Voting System Vulnerabilities

Computer-based voting systems (as well as other distributed computing systems) are vulnerable to attack at three main points: the server, the client, and the communications path. *Penetration attacks* target the client or server directly whereas *denial of service (DOS)* attacks target and interrupt the communications link between the two. Each target and attack will be examined below.⁶

3.1.1 The Client and Server

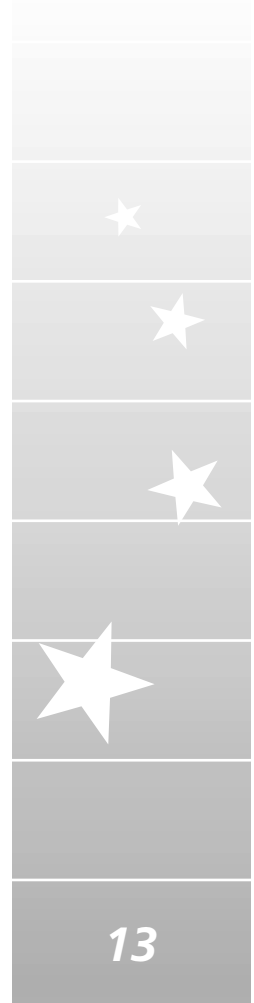
Penetration attacks involve the use of a *delivery mechanism* to transport a *malicious payload* to the target host in the form of a *Trojan horse* or *remote control program*. Once executed, it can spy on ballots, prevent voters from casting ballots, or, even worse, modify the ballot according to its instructions. What makes the latter threat particularly insidious is that it can be accomplished without detection, and such security mechanisms as encryption and authentication (e.g., secure socket layer [SSL] and secure hypertext transport protocol [https]) are impotent against this kind of attack in that its target is below the level of abstraction at which those security protocols operate (e.g., the operating system or browser).⁷ Virus and intrusion detection software is also likely to be powerless against this threat because detection mechanisms generally look for known signatures of malicious programs or other signs of unauthorized activity. These stealth attacks generally emanate from unknown or modified programs, and alter system files to effectively “authorize” the changes made (after which they might disable further virus protection). The attacks could originate from anywhere in the world, including locations beyond the reach of U.S. law enforcement.

These malicious payloads can be delivered either through some input medium (e.g., floppy or CD-ROM drive), download, or e-mail; or by exploiting existing bugs and security flaws in such programs as Internet browsers. Activation need not be intentional (e.g., double-clicking an icon), but can also occur by executing compromised code that users intentionally download from the Internet (e.g., device drivers, browser plug-ins, and applications) or unknowingly download (e.g., ActiveX controls associated with Web pages they visit). Even the simple viewing of a message in the preview screen of an e-mail client has, in some cases, proved sufficient to trigger execution of its attachment.

A Trojan horse, once delivered to its host and executed, might be activated at any time, either by remote control, by a timer mechanism, or through detecting certain events on the host (or a combination of all three). If such a program were to be widely distributed and then triggered on or about Election Day, many voters could be disenfranchised or have

⁶ Much of the material for this discussion has been contributed by David Jefferson of Compaq Systems Research Center and Avi Rubin of AT&T Research Labs.

⁷ Currently, there is no effective way to prevent such attacks on any of the common platforms (i.e., PCs, Macs, and handhelds) running any of the common operating systems (e.g., Windows xx, MacOS, Linux, WinCE, Palm OS). A new generation of hardware is needed to properly address this problem—something that will require at least several years, since such standards and devices are not currently in active development.



their votes modified. Attacks do not have to be confined to individual or random voters, but can be targeted on a particular demographic group. Remote control software⁸ introduces a similar concern in that the secrecy and integrity of the ballot may be compromised by those monitoring the host's activity.⁹

In principle, poll site voting is much less susceptible than remote voting to such attacks. The software on voting machines would be controlled and supervised by elections officials, and would be configured so as to prevent communication with any Internet host except the proper election servers. Election officials and vendors could configure voting clients so that voters and poll workers would be unable to reboot the machines or introduce any software other than the voting application. Careful monitoring of the system could reduce the risks even further. Opportunities for attack and insider fraud, however, would still exist, especially since voting jurisdictions may have difficulty getting the reliable technical support they need to administer their system properly.

3.1.2 The Communications Path

The communications path refers to the path between the voting client (the devices where the voter votes) and the server (where votes are tallied). For remote voting, this path must be “trusted” (secure) throughout the period during which votes are transmitted. This requires both an authenticated communications link between client and server, as well as the encryption of the data being transported to preserve confidentiality. In general, current cryptographic technologies, such as public key infrastructure, are sufficient for this latter purpose, assuming the standards required to run such technologies are met. Maintaining an authenticated communications linkage, however, cannot be guaranteed.

Research Issues—Voting System Vulnerabilities

- **Defense/verification against insider fraud for poll site voting**
- **General defenses against Trojan horse attacks and malicious use of remote control software**
- **Specific design of secure voting platforms and networks**
- **Defenses against denial of service attacks**
- **Defenses against spoofing (fake voting sites)**

Perhaps the most significant threat in this regard is a denial of service (DOS) attack, which involves the use of one or more computers to interrupt communications between a client and a server by flooding the target with more requests that it can handle. This action effectively prevents the target machine from communicating until such time as the attack stops. A refinement of this technique is referred to as distributed denial of service (DDOS) in which software programs called *daemons* are installed on many computers without the knowledge or consent of their owners (through the use of any of the delivery mechanisms referenced above), and

⁸ Examples include the commercial products PC Anywhere, LapLink, Timbuktu, and the cracker tool Back Orifice

⁹ In many respects, remote control software is the same as a Trojan horse in that it can spy on or alter ballots, or prevent them from being cast altogether. The difference is that such software is generally developed for legitimate business purposes.

used to perpetrate an attack (figure 2). In this manner, an attacker can access the bandwidth of many computers to flood and overwhelm the intended target.¹⁰

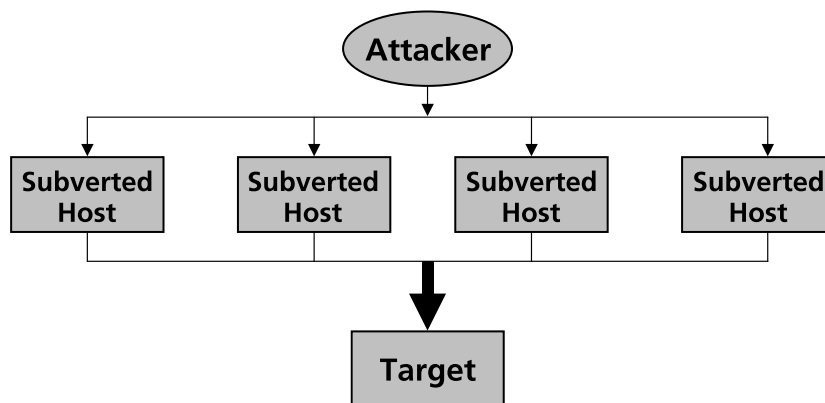


Figure 2: A distributed denial of service (DDoS) attack. This variation of a denial of service attack permits an attacker to seize control of a large amount of bandwidth and launch an attack. First, the attacker subverts a large number of other Internet hosts and installs a Trojan horse program on them that allows the attacker, at any later time, to remotely control the hosts. Later, at the time of the attack, the attacker's computer sends commands to all of the hosts, ordering each to launch an attack against the target, which could be a voting server or an ISP, at the same time. While none of the hosts could successfully mount a successful attack individually, the combined effect can saturate the target's communication link and cut off its access to the Internet.

Currently, there is no way to prevent a determined DOS attack, or to stop one in progress, without shutting down unrelated and legitimate communications—and even then it may take several hours of diagnosis and network administration time. While research is currently being conducted to find ways of limiting this threat, no solution has yet been identified.

For poll site voting, these threats can be avoided by designing the voting clients with the capability to function even if communication between the precinct and the server is lost without warning and never re-established. Accordingly, these systems must, in effect, include the functionality of a DRE (direct recording electronic) system and be able to revert to DRE mode without losing a single vote.¹¹ If the voting clients act as DRE machines, and use the Internet to transmit votes when it is available, then poll site voting systems are not vulnerable to denial of service attacks. Even if the path is totally corrupted, because the votes have been accumulated correctly in the vote clients, one can still recover after the fact from any communication problem. The philosophy is not to rely on the reliability or “security” of the communications link.

This approach is not feasible for remote voting systems because it is not practical or desirable for PCs to emulate all the characteristics of DRE systems. One does not want to store

¹⁰ The reason DDOS attacks are so effective is that the attacker, in effect, controls the combined bandwidth of all the systems that are infected with daemons, making it possible to overwhelm even the most sophisticated targets (e.g., Yahoo, eBay, CNN).

¹¹ In this manner, poll site clients could store cast ballots and upload them to the server after the attack or, if necessary, transmit them physically in secured tamper-proof memory modules.

votes on remote PCs because of the possibilities it would create for vote selling or coercion. It is simply not reasonable to expect voters who were unable to connect to the server due to a DOS attack to physically carry their votes to the election office for tallying.

Remote voting systems will also have to contend with an attack known as spoofing—luring unwitting voters to connect to an imposter site instead of the actual election server. While technologies such as secure socket layer (SSL) and digital certificates are capable of distinguishing legitimate servers from malicious ones, it is infeasible to assume that all voters will have these protections functioning properly on their home or work computers, and, in any event, they cannot fully defend against all such attacks. Successful spoofing can result in the undetected loss of a vote should the user send his ballot to a fake voting site. Even worse, the imposter site can act as a “man-in-the-middle” between a voter and the real site, and change the vote. In short, this type of attack poses the same risk as a Trojan horse infiltration, and is much easier to carry out.

3.1.3 *Balancing Security and Other Interests*

While a main argument in support of Internet voting is the potential increase in convenience, the primary arguments against Internet voting are security concerns. There is a fundamental tradeoff between security and convenience at a given level of technology. Many of the promises of remote voting disappear once security requirements are imposed. Measures that enhance security are often more difficult to use, and require newer and more expensive technologies (e.g., smartcard readers, biometric authentication devices, and cryptographic devices). Over time, as newer technologies become familiar and well integrated into commonly used systems, the trade-off between security and convenience can improve. At the same time, however, new threats may emerge, requiring stronger and less convenient security measures.

Internet voting systems will depend on election personnel (at poll sites) or voters (at remote locations) to ensure that the hardware and software standards provide the needed levels of security. While this task may be daunting for specialists at the poll site, it would be most problematic for remote voters who may possess little or no technical understanding and whose budgets do not allow them to upgrade as necessary. Some social scientists at the workshop suggested that the amount of information required to cast an informed vote, the length of many ballots, and the frequency of elections in the United States already pose a high burden on voters, and that the need to learn additional technical skills would cause many to reject new systems. If only the most technically sophisticated are able to vote securely over the Internet, significant policy questions about equality of access to voting are raised (see section 4.2 on *Voter Access*).

Given the problems associated with the current generation of personal computers, are there alternative, specialized devices that might address some of these concerns? Wireless handheld appliances with “software-closed” architectures¹² offer some promise for solving many of the security problems inherent in the general-purpose processors contained in most clients. In addition, such devices are mobile and might offer a dual use capability—both as a voting mechanism and a telephone, for example. However, there are significant obstacles: first, user interfaces are currently limited in terms of display area, color, and resolution, as well as text input capability; second, such devices may easily be lost or stolen,

¹² “Software-closed” architecture refers to the inability for users to upgrade, add to, or alter in any simple way the software contained within a machine.

necessitating that they be equipped with smartcard or other voter authentication mechanisms; and third, the cost of providing (and replacing) these devices to registered voters could be prohibitive.¹³ Research is needed to determine the viability of this path.

3.2 Reliability

Whereas security refers to the resistance of a system to deliberate, intelligent, or interactive attack, reliability focuses on the questions of a system's ability to perform as intended, in spite of apparently random hardware and software failures. For example, a computer memory failure could result in the loss of recorded votes. The viability of electronic voting rests, in part, on the ability of system designers and elections officials to incorporate redundancy into any deployed voting system and to develop contingency plans for possible failures.

Research Issues—Reliability

- **Design of voting clients (poll site and kiosk) to capture votes accurately in redundant, nonvolatile storage**
- **Technical and procedural methods for increasing reliability of remote voting systems**
- **Voter behavior in response to voting system failures**

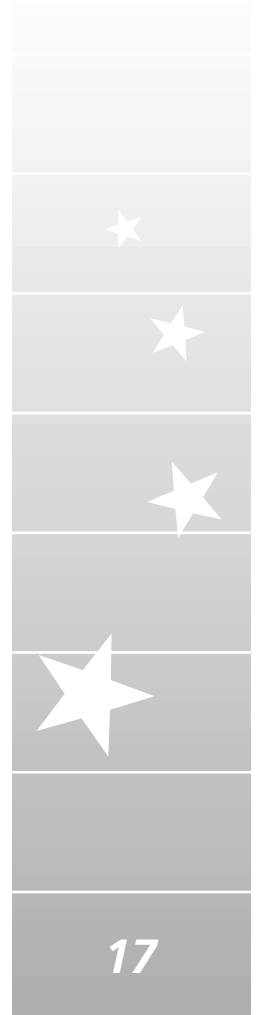
Voters must be able to cast their ballots despite technical difficulties; otherwise many may be disenfranchised. For poll site or kiosk Internet voting, clients should be capable of storing cast ballots and uploading them to the server in a batch at a later time. As discussed previously, this capability would reduce the vulnerability of such voting systems to attack since it would be unnecessary to link the clients to the server until such time as the voting period has expired.

With remote Internet voting, ballots cannot be stored on client computers for ballot secrecy reasons—if such a record is maintained, vote spying and vote selling is facilitated. As a result, reliability of the communications path and election servers is much more critical. A variety of kinds of failures could disrupt remote Internet voting, including server manager mistakes, network congestion or outages along the path the ballot takes, power failures, and the variety of malicious acts described above. Parts of the Internet infrastructure, including routers and domain name servers might also be subject to attack or failure. Parts of the Internet may fail, or provide much degraded performance during critical election periods. Plans for remote Internet voting need to account for such occurrences.

There are both technical and procedural approaches to address these problems. Multiple back-up servers and redundant Internet service provider (ISP) capacity can exist and stand ready for service should they be required due to malfunction or excess demand. Election periods could also be extended beyond one day in order to limit the effect of any incident that threatens to prevent a person from voting at any specific time.

Much research is required, however, to assess both the adequacy of these approaches and to assess how voters would react to failures of an election system. If voters find that they

¹³ Note that the Amendment XXIV to the U.S. Constitution, which abolished the poll tax, prohibits the imposition of any fee in conjunction with voting.



are unable to vote when they want, would they tend to go to a poll site to vote, try again later, or give up?

3.3 Testing, Certification, and Standards

Consistent with the principles of federalism, the states have administered the testing and certification of voting systems.¹⁴ The manner in which each state exercises this responsibility is based in law, but largely derived from tradition. In general, state officials certify voting systems; however, it is the county that determines which certified system to purchase, and when or if to upgrade, based on its own priorities. As a result, as discussed earlier, many types of voting systems from many manufacturers are currently in use throughout the United States.

Research Issues—Testing, Certification, and Standards

- **Written security and reliability standards for various types of voting systems**
- **Improved test methods for Internet voting systems**
- **Models for continuous testing and certification**
- **Federal/State roles in testing and certification**

Recognizing the need to promote a measure of national uniformity in testing and certification criteria, the Federal Election Commission (FEC) and the National Association of State Elections Directors (NASD) promulgated a set of voluntary standards for voting systems in 1990. These standards specify minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria. They address what a voting system should reliably do, but not how it should meet these requirements. To date, 32 states have adopted these voluntary standards.¹⁵ Due to the rapid changes in voting technology, it is important that these standards for voting systems be updated regularly.

Over the years, as new, more complex systems have been developed and marketed, the regulations and protocols under which they are tested and certified have, by necessity, become more sophisticated. The advent of computerized systems introduced issues of software design and testing, thereby increasing the complexity of both the system and the task of certification.

Until recently, when election officials certified new or significantly enhanced models, they “froze” the system, requiring it to be used exactly as certified.¹⁶ The evolving and distributed nature of Internet systems, however, makes the traditional one-time testing and “freez-

¹⁴ For more information regarding this issue, see section 4.7. *Federal, State, and Local Roles*.

¹⁵ FEC data; some states have additional standards.

¹⁶ The concept of “freezing” systems refers to the practice of elections officials whereby they isolate a given system and verify its performance. Once a system is tested and certified, no modifications can be introduced without requiring a further round of testing and certification. At least some jurisdictions welcome incremental changes to systems and can re-certify the modified system relatively quickly.

ing” of systems inadequate for ensuring the integrity of elections. With Internet voting systems, it is likely that software will frequently need to be modified to fix faulty code, to address new threats, to support new platforms or devices, or to respond to evolution in the security protocols and related technologies. As standards change and new hardware is developed, legacy systems may either fail or be rendered insecure in the fast-paced Internet environment. Moreover, as other Internet systems, such as those used for commerce, become less vulnerable with continuing investment in security technology, voting systems may be seen as insecure by comparison.

With this in mind, the workshop panelists urge the states to move toward and eventually adopt continuous certification programs in which Internet voting systems could be decertified when new threats are identified, and re-certified based on the effectiveness of the measures taken to address their assessed vulnerabilities. The vulnerability of software-based systems to new and ever-evolving threats clearly indicates that certification should no longer be considered a permanent seal of approval.

In addition to assuring that the software is secure and reliable, it is also critical to know that the software in use on Election Day is identical to software that was certified. Very small changes to the software could affect election results. There is a need to guard against any opportunity to insert changes in the software, whether malicious or well intended, after it has been certified (unless it is re-certified). Procedures to assure this need to be developed.

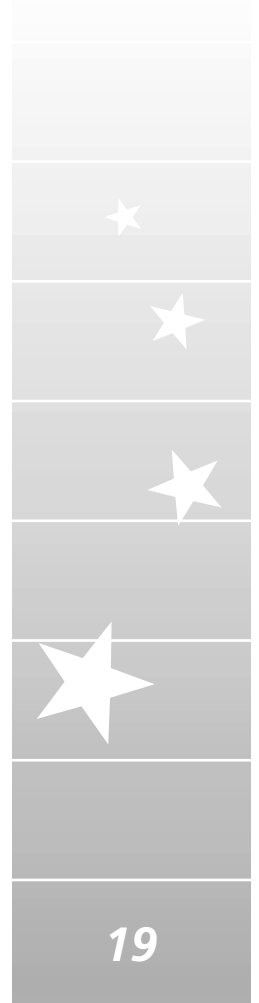
For poll site or kiosk Internet voting (as well as for DRE systems), the testing and certification of systems is a challenging problem. While testing may lead to general confidence in a system, it cannot prove that a system is without flaws or vulnerabilities. Strong verification of such systems is effectively impossible today. For remote Internet voting systems, testing and certification is even more difficult. Such systems would likely rely on third-party components, such as operating systems and browsers, making it hard to define exactly where the system begins and ends, and increasing its vulnerability to attack.

Finally, in light of the mounting difficulty and expense associated with testing and certification of increasingly complex election systems, it makes sense for states to find ways to share the burden. Toward this end, some panelists suggested that the role of the federal government could be strengthened in certain areas to facilitate such cooperation.¹⁷ Studies are needed to examine what Federal and state roles are appropriate, and to identify where constitutional issues arise.

3.4 Specifications and Source Code

An important issue is the extent to which election systems vendors should be required to make details about their systems available to election officials, independent experts, and the public. This affects the ways election systems work with other related technologies, as well as public confidence in the election process.

¹⁷ Using the Federal Aviation Administration (FAA) as an example, it was suggested that the FEC could assume both a coordinating and oversight role in the certification and de-certification of election systems throughout the United States. Another example is the FEC’s role in developing model voter registration postcards for use by the states to conform to the National Voter Registration Act.



Research Issues—Specifications and Source Code

- **Analysis of the tradeoffs between proprietary technology, open architecture, and public source approaches**
- **What would be the effects on security, innovation, interoperability, vendor competition, the range of options available to counties, and public confidence?**

The panel believes that it is important to allow interoperability between different vendor's systems. State and county election officials have limited budgets and will continue to rely in part on legacy voting systems. Interoperability between different vendor's systems is critical in order to maintain competitiveness in the election systems market and to allow the orderly transition from one technology to another. It is also important that developers of specialized clients, such as wireless and interfaces for the disabled, have access to information that will allow them to interoperate with the rest of the voting systems. It is likely that the market for specialized voting devices for the disabled would be too small to be economically viable if developers have to develop separate solutions to work with each proprietary voting system, or if they have to pay license fees to the owners of the proprietary rights in order to bring their devices to market.

To support interoperability, the panelists believe that voting systems should have open architecture—the specifications of all major modules and subsystems of voting systems should be published. This will allow different components and systems that meet the same specifications to interoperate, even if developed by different vendors. Vendors would remain free to create new and better systems, and these would be protected by copyright and patent laws. Certification, however, would require that the system's specifications be made available so that other vendors could make their systems compatible.

Most panelists believe that not only should the specifications of modules and subsystems be published, but that the implementations (i.e. the source code) should be published as well. An election is not fully open if it is based on secret (i.e. proprietary) software. People have a right to know, in as much detail as they are capable of understanding, exactly how their elections are conducted. In addition, experts must be able to scrutinize the system freely for problems. As a general rule, source code is made more secure the more it is scrutinized by others.

While vendors have argued that they need to maintain their technology secrets in order to maintain competitiveness and protect their investment, this investment can be protected in part through intellectual property protections, such as patents and copyrights, and secrecy does not, in any event, prevent copying the technology. Foreign governments and other interested parties can acquire access to the source code for these systems—either through direct purchase of the source code (and foreign governments are unlikely to purchase election systems without access to source code since *their* national security is at stake) or through reverse engineering.

Some panelists noted that there are downsides to making source code public. First, it would facilitate computer criminals in efforts to exploit existing vulnerabilities in the system. Second, while the intended goal of encouraging experts to evaluate the code is sound, such a process could result in many false or erroneous reports of software error, needlessly undermining confidence in the electoral process and diverting the attention of election offi-

cials. Third, public access to source code does not, by definition, translate into more secure systems. In some open source applications, it has taken many years to identify a number of serious problems. Accordingly, “going public” with source code is not an alternative to testing and review by paid professionals.

On balance, however, most panelists believed that the advantages of making source code available for public review significantly outweighed the disadvantages, and urged vendors to disclose the source code of both the client and server sides of their voting systems.¹⁸ Another option, representing a compromise, is to have source code be made available to a panel of experts, perhaps including members of the public selected for their expertise, rather than to everyone. This would help review the code while reducing false alarms.

3.5 Platform Compatibility

System compatibility has long been a vexing problem for the computer industry. It is especially problematic in the realm of election systems due to the high requirements for security and fairness of access. While poll site Internet voting presents some challenges in that voting jurisdictions may operate different platforms, the difficulties associated with remote voting are daunting.

Research Issues—Platform Compatibility

- **Ballot design for different platforms**
- **Demographics and political views of users of different technologies**

Perhaps the most fundamental question in this regard is whether Internet voting systems can be expected to run on all types of platforms (e.g., personal computers, personal digital assistants, wireless telephones, WebTV), operating systems (e.g., Windows xx, MacOS, many versions of Unix, PalmOS, WinCE, JavaOS, BeOS), and browsers (e.g., Microsoft Internet Explorer, Netscape Navigator, Opera, NeoPlanet). In what language(s) should ballots be formatted (e.g., HTML, some version of XML, WML)? Which types of devices (screens, keyboards, pointing devices, communication interfaces, and devices to assist the disabled) should be supported, and how are proprietary device drivers handled? How should ballots be designed from a single source base so that they can both be easily navigated and presented similarly on paper, punch cards, and on all supported electronic platforms?

Supporting all of these platforms adds significantly to the complexity of the system, and greatly increases the cost of testing and certification. However, the failure to do so could result in differences in access to voting among different groups and, because users of different operating systems or browsers may vote somewhat differently, could affect the outcome of elections. Moreover, all of these systems can be expected to evolve considerably between election cycles, leading to the need for continual development, testing, and certification, as well as the attendant costs.

¹⁸ However, a few panelists suggested that the source code of universally-verifiable, protocol-based applications might be exempted from public disclosure if such certification were available.

3.6 Secrecy and Non-Coercibility

A critical criterion for voting systems is that they maintain the secrecy of the ballot. In democratic elections, the link between the ballot and the voter must be irreversibly severed to ensure that votes are cast freely. Voters must be unable to prove how they voted, in order to reduce the risk of coercion or vote selling.¹⁹ This is one key difference between voting and electronic commerce transactions. In the latter, both parties are supposed to know the identity of the other and all details of the transaction.

Research Issues—Secrecy and Non-Coercibility

- **Methods and protocols to reduce ability to buy, sell, or coerce votes**
- **Audit trails that do not permit association of the voter with the vote**

An important factor affecting the degree of secrecy in any election is whether the balloting—either conventional or electronic—is conducted remotely or at a poll site. In a controlled environment, such as the poll site, election officials and observers can ensure that people cast their ballots unimpeded by any outside influence. Conversely, remote voting—over the Internet or by conventional absentee ballots—can be observed, opening the door to the possibilities of vote selling and coercion. Kiosk Internet voting may fall either closer to poll site voting or closer to remote voting, depending on the physical environment of the kiosk and how it is monitored.

Remote Internet voting also poses additional threats to the integrity of elections beyond those of paper absentee ballots. First, for those who access the Internet from their workplace, systems administrators can often monitor or record the activity at each workstation. This presents an opportunity for monitoring and coercion that is unlikely to occur with paper absentee ballots. Second, the distributed nature of the Internet could facilitate schemes for large-scale, automated vote selling or trading that would be more difficult with paper absentee ballots.

While technical approaches to reducing the likelihood of coercion and fraud are possible, it is difficult to assess their effectiveness. One way to mitigate this problem would be to provide voters with the ability to vote multiple times, and have only the last vote count. This would complicate any effort to coerce or buy votes in that the perpetrator could not be assured that the voter did not later change his or her vote. Such a scheme might have many practical problems, however, such as encouraging additional last minute voting and complicating audit trails or recounts. Absent a controlled environment, there is no way to guarantee that some degree of coercion will not occur, especially within families, or in institutional settings such as nursing homes or workplaces.

¹⁹ If voters cannot prove how they voted, buying votes becomes a worthless endeavor in that potential vote buyers would not know what they are buying.

3.7 Comparative Risk

As demonstrated during the 2000 presidential election, traditional methods of voting are not perfect. All election systems inherently possess some degree of risk.²⁰ The degree of risk depends not only on the election system in place, but also to some extent on the type of election and the political culture of a jurisdiction. One would expect high profile elections and elections in jurisdictions with a history of vote fraud to be more likely targets for attack or fraud. One might expect elections for President and other federal office to be more likely to be targeted for attack (and by more sophisticated means) than local school board elections or non-binding referenda. The effect, in terms of public confidence, of a compromised election at the national level would also be correspondingly greater.

Research Issues—Comparative Risk

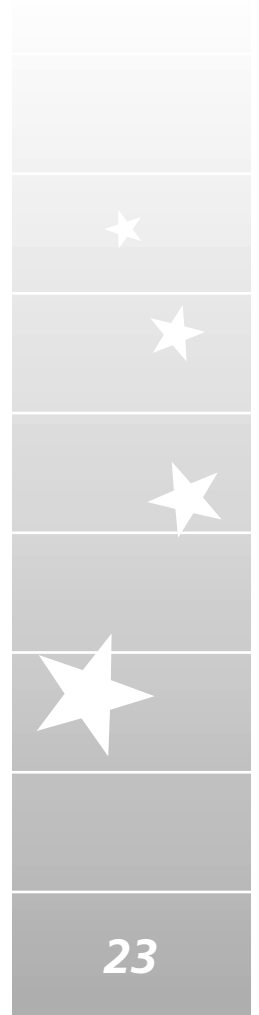
- **Comparative analysis of risks of different voting systems**

This raises the question of how much risk is acceptable for Internet voting (as well as for other electronic voting). Should Internet systems be held to the same standard as current conventional systems, or one that is somewhat higher? There is also a need for detailed analysis of the comparative risk of different voting systems. Poll site Internet voting appears potentially able to meet currently accepted levels of risk; remote voting, however, does not, at least with current or soon-available technology. The possibility of large-scale automated attacks on remote Internet voting systems leads to a level of risk so high as to be unacceptable.

The FEC is considering how to extend its voluntary standards to Internet voting systems, and will take up the issue in early 2001.²¹ One option is the development of standards based on risk and vulnerability. Since local contests are believed to be less likely to be subjected to sophisticated attacks, and the consequence of election failures would be smaller, it might be appropriate to have somewhat less stringent security requirements for municipal and county elections than for national elections. Similarly, there might be small populations of people, such as overseas voters, for whom the benefits of Internet voting would be substantial while the risks to the overall election of allowing them to vote by Internet would be small.

²⁰ The concept of risk, as used here, is a measure of both the likelihood and the consequence of an adverse event. The risk of an election might be considered to be the total of the probability times the consequence of each possible election system's failure mode.

²¹ Discussion between Richard M. Schum and Penelope Bonsall, Director of Election Administration at the FEC.



4. Social Science Issues

4.1 Voter Participation

With barely half of the eligible population voting in the 2000 presidential election, following a four decade-long decline in participation, voter turnout continues to be an issue of paramount interest and concern to both academics and policymakers. Over the past few years, a variety of interests have argued that Internet voting will increase voter participation, particularly among under-represented groups such as youths, the elderly, the disabled, and persons abroad. They contend that, by addressing two main obstacles to voting—convenience and mobility—Internet voting will attract new and disaffected voters to exercise this right and privilege.

Research Issues—Voter Participation

- **Effect of remote Internet voting on turnout in public and private elections**
- **Effects of kiosk voting on participation**
- **Influence of campaigns and on-screen advertising on participation in Internet elections**

Many social scientists studying the pattern of decline in voter participation believe that it is unwarranted to assume that Internet voting will increase turnout. Previous reforms designed to make voting more convenient—simpler registration procedures, liberal absentee balloting, extended voting times, voting by mail—have had very little if any effect on turnout levels and virtually none on the composition of the electorate. Reducing further the costs of voting may well pale in significance compared with the extremely low benefits of voting perceived by many nonvoters. Research suggests that information, motivation, and mobilization are much more powerful forces shaping voting participation than convenience. Further research, however, may reveal a greater turnout potential from Internet voting than is now apparent.

In many of the private and party-run elections already conducted by Internet voting, there have been signs of increased turnout. Anecdotal evidence suggests substantial increases in turnout in college elections when students are permitted to cast ballots from their wired dormitory rooms. The 2000 Arizona Democratic party primary, in which a substantial number of votes were cast remotely over the Internet, saw an increase in turnout over its 1996 counterpart, but a variety of differences between the two party-run elections make comparison difficult.²² More research is clearly needed to determine the proximate cause of this phenomenon and its broader applicability.

A number of possibilities associated with the Internet's impact on voting have been advanced. One possibility is that the convenience, attraction, and familiarity of the

²² In the 1996 primary, President Clinton ran unopposed whereas the 2000 primary was contested for part of the voting period. There was substantial publicity to the fact that election was run over the Internet, as well as substantial efforts by the election system vendor to mobilize the vote. Total participation was still less than ten percent of registered Democrats.

Internet, especially among young voters, would lead to a sustained increase in turnout. Another possibility is that Internet voting may initially attract voters due to the popularity of the medium and the publicity surrounding the election. However, this affinity may diminish over time if the motivation for voting is primarily novelty. Another possibility is that Internet voting could actually depress voter participation in the long run if it is perceived to undermine the legitimacy of the balloting process or feelings of civic participation (see section 4.6. *Community and the Character of Elections*). It is also possible that remote Internet voting would be such a significant departure from previous forms of voting that a new body of research on what motivates voters will be needed.

While convenience and mobility are clearly appropriate policymaking concerns, they do not stand alone. For example, it may be possible to make voting too convenient. Suppose one could vote for a given candidate immediately upon receipt of a targeted campaign message by clicking a link embedded into the body of the e-mail. How would this “vote for me now!” type of vehicle affect campaign strategies, political activism, or deliberative democracy? Research is needed on these the kinds of questions.

Most attention on the potential for Internet voting to affect turnout has focused on remote Internet voting. Poll site and kiosk voting offer voters some potential benefit in increased convenience, such as the ability to cast their ballot from many more places. One would expect that this more modest increase in convenience would have a smaller affect on turnout compared to remote Internet voting.

4.2 Voter Access

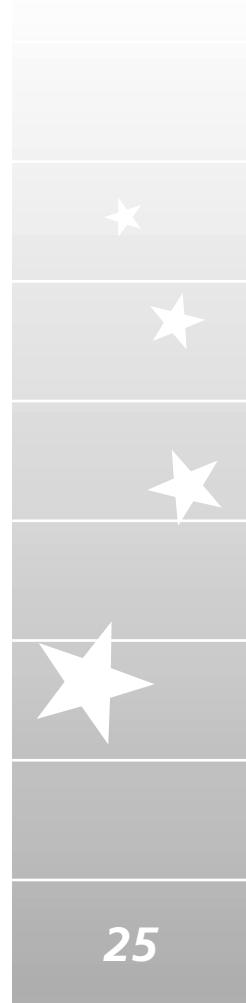
How Internet voting would affect the turnout of different demographic groups, defined by race, education, age, party affiliation, or geographic location, in each district is an important concern to policymakers. The adoption of any voting system that might limit the electoral strength of any particular group would likely be subject to legal challenge.

Research Issues—Voter Access

- **Demographics of Internet access and use**
- **Public attitudes about computers and Internet voting**

Poll site Internet (or DRE) voting could be expected to have small but possibly significant effects on the access to voting by different demographic groups. Voters would have equal physical access to the voting stations, but demographic groups with less familiarity with computers might find some types of electronic voting to be more difficult and intimidating. The adoption of Internet voting systems could also have a disproportionate impact on certain groups through other means. If, for example, Internet voting systems were to have a lower rate of failure (e.g., under-votes, over-votes, or other rejected ballots) than the systems they replace, and if wealthier jurisdictions move to Internet voting first, then the voters in those areas would be slightly favored.

Poll site Internet voting also could enable people with a variety of disabilities to vote without assistance. A much richer and more capable variety of disability-accessible voting machines is possible on a computerized platform than with any other voting technology.



Remote voting could be expected to have a much more significant impact on access to voting. Voting would be made easier for people who have ready access to Internet-linked computers. At present, individuals with higher levels of income and education are more likely to have Internet access; whites more so than other races; and people over 55 less so than their younger counterparts. These trends are changing rapidly, however. Women and the elderly, in particular, have made remarkable progress in getting online. By the time remote voting becomes a viable option, the demographics of Internet access will have changed. Policymakers need to have access to reliable statistics that reflect this. Moreover, if the security requirements for remote Internet voting demand that voters have specialized or high-end computing systems, this will also favor the most advanced and wealthiest computer users.

4.3 The Election Process

Internet voting is likely to lead to changes in the way elections are held, in the way elections and ballot counting is monitored, and in the role of recounts. It is also likely to change many other aspects of election administration.

Research Issues—The Election Process

- **Transparency, recounts and public confidence in electronic voting systems**
- **Effect of Internet voting on all aspects of election administration**

In most jurisdictions today, Election Day is a defined period of perhaps twelve hours during which voters irreversibly cast their ballots one time. As described earlier, this traditional way of voting is already breaking down in many jurisdictions through voting by mail, voting at satellite locations, and early voting. Internet voting is likely to expand and accelerate these trends. Extended voting periods are one way to reduce the vulnerability of Internet voting systems to technical failures or attacks (by allowing time to recover if the system goes down). Internet voting could also make it possible to allow for people to vote part of their ballot at one time, and then return to complete their ballot at another time (known as partial ballot voting). Moreover, a possible way to reduce the risk of coercion and vote selling with remote Internet voting would be to allow people to cast multiple ballots and to have only the last ballot count. This would reduce the incentive to buy or coerce votes because it would be hard to know that the vote that was bought or coerced actually counted. Internet voting could enable and generate the demand for such changes in the election process. Computerized voting (whether Internet or not) makes it feasible to adopt exotic voting systems, such as “instant runoff” elections.

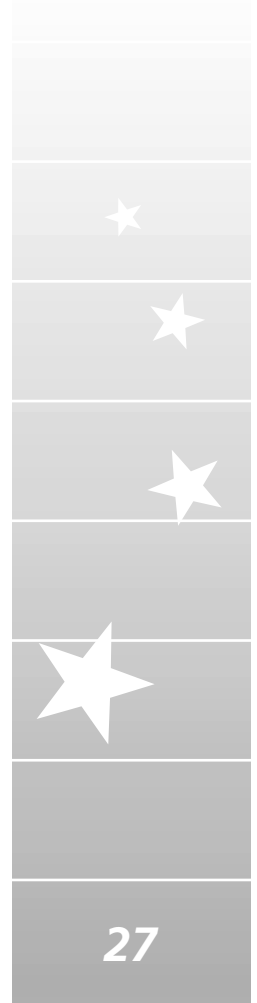
Each of these possible changes would require careful analysis. Longer voting periods may raise costs, especially if the poll sites are open longer. And there are likely to be many practical complications to allowing partial or multiple votes. Moreover, each of these changes could be expected to lead to further changes by political campaigns to try to capitalize on the changes.

Public confidence in the manner in which ballots are counted is fundamental to the legitimacy of the electoral process—a lesson relearned during the controversial vote counting in Florida in the 2000 Presidential election. Internet voting is likely to lead to changes in how the public maintains confidence in the integrity of elections. Public elections generally use observers from different parties to monitor elections and vote counting. Several officials with differing or conflicting interests are required to validate the results of an election. Unlike more conventional voting systems, Internet systems pose a problem (shared with DRE systems) in that the tallying process is not transparent. Though election procedures may require several officials and/or observers to activate a “key” to initiate tabulation, this does not ensure the accuracy of the results. Accuracy depends upon a variety of factors, such as the integrity of the system, the vulnerability of the hardware, software, and networking medium, and skilled personnel to operate and troubleshoot the system, none of which is transparent to monitoring officials. With electronic voting systems, public confidence in the election relies on trust in technical experts instead of a transparent process.

A related issue is what would actually constitute a recount for Internet voting systems? Would it suffice to “turn the key” yet again and regenerate the same answer? Could public confidence in the legitimacy of the election process be maintained in this manner? Would such a “recount” satisfy state and federal law? Many states election statutes require an actual physical counting of individual ballots. DRE systems currently in use generally meet this requirement by printing out ballots based on the electronic tally, which simply guarantees that any system error will be reflected in the printed ballots. While Internet systems can adopt this same approach, it is unclear whether election officials will continue to accept this as sufficient.

Internet voting also affects the election administration process in many other ways. Voter education, communications with voters, recruitment and training of poll workers, identification and designation of polling places, storage and maintenance of voting equipment, creation and production of ballots, and many other aspects of election administration can be expected to change with a move to Internet voting. The effect will be different, depending on whether Internet voting is an add-on to existing voting methods or a replacement.

Another issue raised by Internet voting is how to manage election data. Administration of elections not only requires voter registration databases but also produces data that determines the winners of elections. This data can potentially be analyzed by political consultants, and if combined with other data, might be useful to a variety of marketing firms. What rights, if any, would election systems vendors have to this data? Would it be allowable for election officials to recoup costs by selling election-related data? What are the risks of misuse of databases by persons authorized to work with them? Are there benefits of providing some form of this data to social science researchers? Procedures for how to handle and use this data merit further discussion.



4.4 Voter Information

While the act of voting is important to the political process, the casting of an informed vote is the ideal of American democracy. Toward this end, it is often suggested that the Internet can enhance the quality of the vote by delivering to consumers the information they require in order to educate themselves on the issues. While this issue is largely separable from the Internet voting itself, one of the arguments advanced for remote Internet voting is that it would enable people to conduct research on the candidates and issues as they vote.

Research Issues—Voter Information

- **How do voters use Web-based voter information?**
- **Does Internet voting affect this behavior, or would it be affected by it?**

The wave of information that has resulted from an exponential growth in the channels of distribution over the past few decades has greatly increased the sources of information available to voters. Conventional media outlets no longer exert the same level of control on what information is available to the public. With the barriers to entry in the market at an all-time low, virtually anyone with a PC is now able to “publish.” But this freedom has not come without a price: the consistency and quality of the information has suffered and consumers are often unable to determine its reliability.

The value of remote voting can be seen as combining the convenience of voting from home over the Internet with access to a wide variety of information relevant to the issues pertaining to an election. Yet, with so many sources of information, how well can voters distinguish between what is credible and what is not? This is an issue that goes beyond Internet voting.

4.5 Deliberative and Representative Democracy

Some people believe that one of the principal advantages of remote Internet voting is that in the long run it could facilitate more direct involvement by citizens in the decisions of government. Others, including many of the workshop panelists, view this as a potentially dangerous trend.

Research Issues—Deliberative Democracy

- **Effects of poll site, kiosk, and remote Internet voting on the market for direct democracy.**

Among the principal aims of the Framers in crafting the United States Constitution was the establishment of a system of government that limited the excesses of direct democracy and promoted deliberation over efficiency. Accordingly, they adopted a federal framework, separated the powers of government, set up an elaborate system of checks and balances, and instituted a bicameral legislature. This elaborate system slowed down lawmaking and

encouraged deliberation, debate, and consensus building. Most state governments have also adopted this model.

The emergence of remote voting could, in the long run, undermine the deliberative nature of our political system by enabling interest groups to bypass the legislative process in favor of direct referenda and initiatives at the various levels of government.²³ Legislators, fearing the political consequences of certain votes, might choose to pass them on to the people in weekly or monthly balloting, forgoing in the process the policy expertise and reflection that are inherent to the legislature.²⁴ By reducing the economic and logistical barriers associated with poll site balloting, remote voting might facilitate these scenarios in that it would allow for elections to be conducted more frequently than at present. Instead of putting a few referenda to vote each year, it could become easy and cheap to do hundreds.

Though efforts to expand the scope of remote voting from electing representatives to acting on legislation appear well-motivated and democratic in nature²⁵, the risk they may pose to the protection of the minority and to deliberative democracy in general is significant. Accordingly, the workshop panelists encourage research aimed at understanding the long-term consequences of remote voting on deliberative democracy.

4.6 Community and the Character of American Elections

The act of voting in the United States is more than simply a means by which to elect officers of government; it is a constituent element of representative democracy and a ritual coming together of concerned citizens. At this one time, all citizens who enter the voting booth are of equal stature—each casts one vote notwithstanding their differences in race, education, occupation, or net worth.

Research Issues—Community and the Character of American Elections

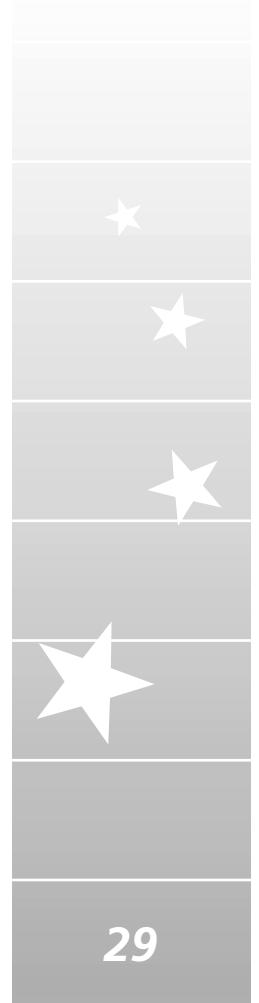
- Effects of vote-by-mail on social capital
- Effect of Internet in general on civic participation and social capital

While poll site voting might have little effect on the sense of community attributable to current voting conventions, remote voting represents a significant departure from the past in terms of the type and quality of civic engagement. By enabling a select group—perhaps

²³ David S. Broder in his book, *Democracy Derailed*, argues that these “democratic” instruments of public participation in the legislative process actually undermine the deliberative nature of our representative democracy and pose a threat to the integrity of our political process.

²⁴ Another possibility is that remote voting might promote the idea of recall elections at all levels of government. Currently, no such vehicle exists for federal offices, though some states and localities do provide for such initiatives.

²⁵ Former U.S. Senator Michael Gravel (D-AK) is currently heading up two organizations, Philadelphia II and Direct Democracy, whose mission is to promote direct democracy initiatives at the federal level in an effort to address the public’s loss of faith in government. Other groups are promoting similar efforts.



the more affluent and more educated—to opt out of going to the polls, the level of social cohesion within a community may be affected.

There are, however, many ongoing changes in society that affect social cohesion both positively and negatively. There is debate, for example, about whether the Internet in general builds social cohesion by enabling better communication among community networks, or undermines it by replacing face-to-face social groups with virtual ones. It is unknown whether the effects of Internet voting on social cohesion would be significant in the context of larger social changes.

The vote-by-mail system adopted by Oregon could be expected to have similar effects to remote Internet voting in this regard. By eliminating the need to go to the polls, these alternative voting mechanisms promote the interest of the individual (i.e., convenience) over that of the community (i.e., civic participation). Vote-by-mail system may serve as a proxy for remote voting, providing researchers with the ability to study the effects of adopting such a system.

4.7 Federal, State, and Local Roles

Consistent with the principles of federalism, the principal authority and responsibility for administering elections is entrusted to the states. Each state adopts its own electoral requirements and standards, and generally delegates the actual conduct of elections to elected county officials. As a result, there is a wide variation in the standards, technical capacity, and culture of administration of each county jurisdiction. Voting systems are purchased at the local level; however, the certification of these systems is a matter reserved to state election officials—most frequently acting under the authority of the Secretary of State.²⁶

Research Issues—Federal/State/Local Roles

- **The appropriate role of the federal government in state-administered elections**
- **Risks and benefits of centralization in voting systems**

Due to their considerable cost and the limited resources of counties, voting systems are frequently purchased from the lowest bidder, and often used for decades after their initial acquisition. For example, in some areas, 1930s-era, mechanical lever machines are currently in service. While the problems associated with the continued use of such vintage systems were previously thought to be little more than an inconvenience, the closeness of the 2000 presidential election drew attention to important flaws in some of these systems.

Some have suggested that some form of Internet voting may be the solution to many of the problems presented by conventional voting systems. In the contested 2000 presidential election in Florida, however, the main problems were the absence of standards for deciding which improperly marked votes would be counted, as well as a required recount structure that did not fit well with the certification timelines. These issues, more than the voting technology, contributed to the controversy.

²⁶ For more information regarding this issue, see 3.3. *Testing, Certification, and Standards*.

In any case, the current distribution of authority among counties, states, and the federal government does not appear to lend itself—at least at present—to the use of Internet voting systems in statewide or national elections. To realize the full economic and efficiency benefits of Internet voting, the administration of voting systems must be centralized to some degree. For example, to allow voters to vote from any poll site in a state would require a substantial degree of state-wide cooperation on Internet voting and registration systems. Internet voting could also lead toward greater national level cooperation and standardization in voting systems.

There are risks as well as potential benefits in greater centralization or harmonization of voting systems. One advantage of the current decentralized system is that it is very difficult to conduct election fraud at a large scale. An attack on a voting system in one jurisdiction is unlikely to affect election results in a neighboring jurisdiction that may use a completely different system of voting. Greater centralization or even greater consistency among election systems makes it easier to disrupt or influence elections on a large scale.

4.8 Legal Concerns

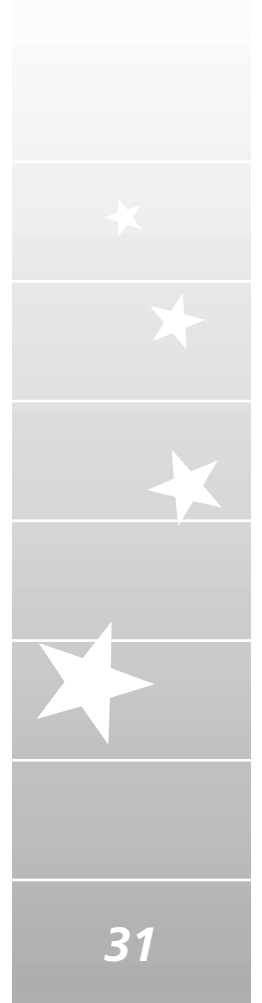
There are a wide variety of legal issues raised by the prospect of Internet voting. The advent of Internet voting will likely require substantial review and reform of our federal and state election laws. Current law is generally predicated on conventional voting systems and the types of abuses associated with each, and is not sufficient to address the many new elements and risks introduced by Internet voting. One concern relates to the definition of recounts, as discussed earlier.²⁷ Another concern relates to electioneering laws. For example, while existing laws restrict electioneering near polling places, they do not address the issue of on-screen advertising (in conjunction with remote voting); effectively, therefore, they enable such practices to occur until such time as these laws are revised. Voters may access voting Web sites through Internet service providers that provide ads on the viewer's screen. These ads could link voters to spoof Web sites that could change votes or make voters think they are voting when they are not. The ads could also facilitate vote selling and trading schemes. There are many possibilities for voting abuse that can be created as a consequence of using the Internet as a voting medium, and many of these may require regulation or new legislation.

Research Issues—Legal Concerns

- **International law with respect to Internet voting attacks and fraud**
- **Liability for failures of Internet voting systems**
- **Application of electioneering laws to Internet voting**
- **Effect of e-commerce-related policies and laws on Internet voting, such as restrictions on strong encryption or the ability to reverse engineer software**

Another major issue is jurisdiction. The Internet is an international medium not governed by any sovereign entity. While cases of vote fraud have historically involved individual or small groups of violations occurring within a jurisdiction that rarely affected the outcome of an election, Internet voting introduces the possibility of automated fraud and attacks that

²⁷ For more information on this issue, see section 3.3. *The Election Process*.



can be perpetrated across national boundaries. Acts of fraud or other abuses that are committed outside the United States may not be subject to prosecution under state or federal law, and/or may be impossible to enforce absent a treaty between the respective jurisdictions.²⁸ Foreign laws may serve to complicate this problem by interposing standards and criteria different from U.S. law. Finally, existing statutes and administrative regulations may not even apply to Internet voting in that they often reference conventional voting systems and processes associated with them.

Any effort to address these risks would likely require the enactment of reciprocal agreements among nations to effect multinational jurisdiction and enforcement actions such as apprehension and extradition of suspects. At a minimum, international law must require each nation to respect the democratic processes of other nations, and protect them from interference by those who seek to undermine their continued viability.

A separate legal issue raised by Internet voting is that of liability. Historically, election officials have assumed much of the responsibility for any failure of voting systems. This seemed reasonable since, it was argued, these machines were in their charge and problems were a direct result of their actions. As voting systems rely increasingly on software and network technologies, it is no longer possible for election officials to be personally knowledgeable or accountable for possible failures in the system. With current voting systems, errors are likely to be on a relatively small scale. Internet voting, however, substantially increases the scale of potential problems. Policymakers must concern themselves with the possibility of a discovering a software glitch only after it had changed the results of an election. How would this be handled and who would be liable? What effect would it have on public confidence in the legitimacy of the process?

Specifically with regard to remote Internet voting, a number of other legal reforms may be required, such as the enactment of strong laws prohibiting the unauthorized use of digital signatures, and the transference of one's vote. In addition, some panelists argued that existing laws or policies might serve, in some cases, as barriers to developing effective Internet voting systems, including:

- Encryption policy that restricts the use of strong encryption—a barrier to enhancing privacy and verification;
- The Uniform Computer Information Transactions Act (UCITA), which provides legal standing to licensing agreements on shrink-wrapped and downloaded software, and can be interpreted to prevent experts from examining software code for weaknesses or errors;
- The Digital Millennium Copyright Act, which criminalizes some technologies used by security people to find bugs in software.

²⁸ While the United States has begun to employ “long arm statutes” in order to establish U.S. jurisdiction abroad, the issue of enforcement would still present a significant obstacle to protecting the voting process.

4.9 Voter Registration

To exercise their right to vote, citizens must first register with the election authority of the state within which they are domiciled.²⁹ Accurate voter registration lists are important to election integrity—if the names of ineligible (or non-existent) voters are on the registration list, it becomes easy to add fraudulent votes to an election. The 1993 National Voter Registration Act, which had as its purpose to expand voter registration, limited the amount of information states could require in the registration process and also made it more difficult for election officials to purge registration lists. Election officials now believe that the accuracy of voter roles has declined and there are now more ineligible persons on the voter roles than before. As a result, most election officials argue that voter registration systems currently pose the greatest risk to the legitimacy of the electoral process.

Research Issues—Voter Registration

- **Analysis of effects of NVRA on voter registration**
- **Comparative analysis of state voter registration procedures**
- **Issues related to management of digital keys (upgrading, borrowing, selling, theft, duplicate keys)**

Can the Internet be used to improve the voter registration process? The consensus of the workshop was that while it might be feasible for registered voters to update personal information (e.g., changes in address) over the Internet, initial registration would have to occur by other means for the foreseeable future. At the time of registration, each citizen could be provided with a *bona fide* means of authentication, such as a digital signature, to identify themselves during online transactions.³⁰ Purely electronic voter registration would be dangerous because it might enable a third party to fraudulently register large numbers of people using publicly available “phonebook” databases. While the potential benefits of a biometric identification system would be significant, such a database would likely present insurmountable political obstacles with regard to privacy and other democratic concerns.

The advantages of Internet voting linked to online registration are considerable—even if restricted to updates. Such a system could address the problematic jurisdictional issues posed by residence and mobility. Under the National Voter Registration Act, elections officials are required to follow and confirm address changes of voters within a county once registered. An Internet voting and registration system would likely simplify the logistical difficulties associated with updating and purging the voter registration roles, and offer the potential for portable and permanent voter registration without the risk currently posed by traditional registration systems in use throughout the nation.

²⁹ Except in North Dakota, which has no voter registration requirement. Some other states allow Election Day registration.

³⁰ It was suggested that a government office, such as the Department of Motor Vehicles or the U.S. Postal Service, could distribute such mediums of identification—either separately or in conjunction with official government documents.



5. Findings and Recommendations

The following are the findings of the executive committee regarding the feasibility of Internet voting and their recommendations for research.

5.1 The Feasibility of Internet Voting

*P*oll site Internet voting systems offer some benefits and could be responsibly fielded within the next several election cycles. While many issues remain to be addressed, the problems associated with these systems appear likely to be resolvable in the short term. As such, it is appropriate for experiments to be conducted and prototypes deployed in order to gain valuable experience prior to full-scale implementation. This would provide a basis for evaluating poll site voting compared to other voting systems. If found to be preferable to other systems, poll site Internet voting could be deployed in several phases. For instance, voters might first cast their ballots at the precinct level, then from anywhere within the county, and finally from anywhere within the state. The latter step would require registration and voter systems in the different counties to work together.

The next step beyond poll site voting would be to deploy kiosk voting terminals in public places. This path toward greater convenience would enable technologists and social scientists to address the many issues that confront the voting process at each level of implementation. Many issues related to kiosk voting, such as setting standards for electronically authenticating voters, still need to be resolved.

*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.*³¹ The security risks associated with these systems are both numerous and pervasive, and in many cases cannot be resolved using even the most sophisticated technology today. In addition, many of the social science concerns regarding the effects of remote voting on the electoral process would need to be addressed before any such system could be responsibly deployed. For this reason, it is imperative that public officials educate themselves about the dangers posed by remote Internet voting, and the ramifications of failure on the legitimacy of the electoral process.

Internet-based initial voter registration poses significant risk to the integrity of the voting process, and should not be implemented until an adequate authentication infrastructure is available and adopted. While information already in the domain of election officials may be updated remotely, given appropriate authentication protocols, initial registration conducted online cannot establish the identity of the registrant absent the transmission of unique biometric data (e.g., fingerprint or retinal scan) and an existing database with which to verify it.³² Online registration without the appropriate security infrastructure would be at high risk for automated fraud. The voter registration process is already one of the weakest links in our electoral process. The introduction of Internet-based registration without

³¹ However, remote Internet voting may be appropriate in the near-term for special populations, such as the military and their dependents based overseas. Such exceptions should be evaluated on a case-by-case basis.

³² In many states, a mailed-in live ink signature on an affidavit signed under penalty of perjury, serves to authenticate the registrant.

first addressing the considerable flaws in our current system would only serve to exacerbate the risks to which we are already exposed.

The panelists recognize it is possible that advances in technology may be able to address many of the concerns regarding remote voting in the future and, as such, they urge that social and technical experts adopt a long-term research focus in an effort to address these issues responsibly and without political interference.

5.2 Research Issues

There is a large, diverse, and important research agenda for Internet voting. Many panelists believe that there has been inadequate research and analysis related to voting for many years. They believed that due to the lack of attention to these issues, election system failure were possible and even likely. The November 2000 presidential election and its aftermath showed these fears to be well founded. In the wake of the election, there are many calls for change. However, the research base needed to make sound decisions is weak at present.

The workshop raised a large number of issues that require research. There is a need for short-term research related to poll site Internet voting, as well as longer-term research agenda related to kiosk and remote Internet voting. Some of these issues require research of the kind that the NSF typically funds. Other issues require applied research or analysis of the kind that may be more typically performed by consultants, although much of this could be performed by a research center funded by both the NSF and other sources.

There is especially a need for interdisciplinary research, and research that involves both researchers and election officials. The workshop was one of the first times that many social scientists, voting officials, and information technology specialists had come together to address the issues related to electronic voting. Many of the issues require the involvement of technical specialists, political scientists, sociologists, anthropologists, psychologists, communications experts and others.

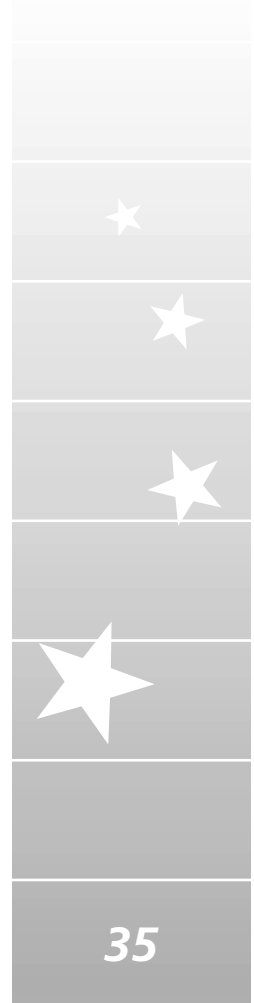
It is especially appropriate to conduct an aggressive program of research and analysis on election issues now. The 2000 Presidential election has brought about a rare opportunity to make reforms in election systems. Many election jurisdictions around the country are currently facing once-in-a-generation decisions on new election systems. It is important that these decisions be based on a solid and current body of knowledge.

It is also likely that there will be substantial public and political pressures to adopt remote Internet voting in the near future, despite the serious concerns of election officials, social scientists, and security and other information technology experts. It is vital, therefore, that research efforts begin immediately so that policymakers will have the requisite information to make responsible decisions regarding the deployment of Internet voting systems.

5.2.1 Voting System Vulnerabilities

There are several security issues related to poll site Internet voting. Research is needed in the following areas:

- Reducing the risk to Internet voting systems from insider fraud, such as through universally verifiable election protocols that allow any knowledgeable individual to verify that an election has been properly conducted.



- Assessing the feasibility of making computers used for other purposes (e.g., in schools and libraries) secure enough for poll site Internet voting, and how that could be accomplished within a certification program.
- Analyzing the cost, benefits, and risks of poll site Internet voting systems compared to those of current and alternative voting systems.

For remote Internet voting, a much broader range of long-term research is needed. Key areas include:

- Development of secure voting platforms and secure networks;
- Defenses against Trojan horse attacks and the malicious use of remote control software;
- Defenses against denial of service attacks;
- Research and development on other possible voting clients, such as specialized voting devices;
- Defenses against spoofing (fake voting sites);
- Defining technical criteria for deciding which of a potentially vast number of systems and platforms to support for remote voting; and
- Avoiding the introduction of bias through the selection of platforms that are more available to some demographic groups than others.

Some of this research may also be useful to e-commerce, as well as other e-government applications, because Internet voting often has stronger technical security requirements than electronic commerce. In many cases, it may be desirable to study legal and administrative approaches, as well as technical approaches, to reduce security risks.

5.2.2 Reliability

Research is needed on how best to design Internet voting systems, both poll site and remote, to be robust with respect to a large number of possible technical failures, including failures of voting clients, the communications path, and servers. Research is needed on architectures for poll-site voting systems in which each precinct has no single point of failure, and has a infinitesimal probability of losing any legitimately cast votes.

The most important reliability consideration of all is that the votes be captured accurately in redundant and non-volatile storage within the voting client. Once that happens, all other failures can in principle be tolerated and recovered from.

5.2.3 Testing, Certification, and Open Source

Studies are needed to define the deficiencies in the current certification process for voting systems, and to develop a model for continuous testing and certification. It is also important to study ways to ensure that software actually used in voting systems is exactly the same as the software that was certified.

Analysis is also needed to study the effects of open source code requirements on innovation, profitability, and public confidence, and the tradeoffs involved with proprietary versus open source code. Most technical panel members believed electronic voting systems should be required to be public source. Studies are also needed to establish and improve test methods for Internet voting systems. Which procedures and protocols should inde-

pendent test authorities follow, both for the main Internet voting system and for add-ons, such as equipment for people with disabilities?

5.2.4 *Design*

Research is needed into the design of voting systems and electronic ballots. One goal is to improve the design of voting systems to make them accessible to people with disabilities. Another goal is to understand how best to design electronic ballots to present choices clearly and fairly to voters. The ordering and placement of candidates and ballot propositions may affect election outcomes. Human factor research is needed to determine how best to design user interfaces and ballots, and how voters respond to alternative ballot designs.

Ballot design is important for poll site voting, but becomes even more critical with remote voting, when ballots will need to appear properly on a variety of computer platforms and screens. Ballot design for small screens will be particularly challenging. It may be appropriate to conduct studies in collaboration with cognitive psychologists, package designers, and computer graphics specialists. It may also prove useful to be able to produce ballot images for many platforms from a single source file so that the ballot editing process is more manageable.

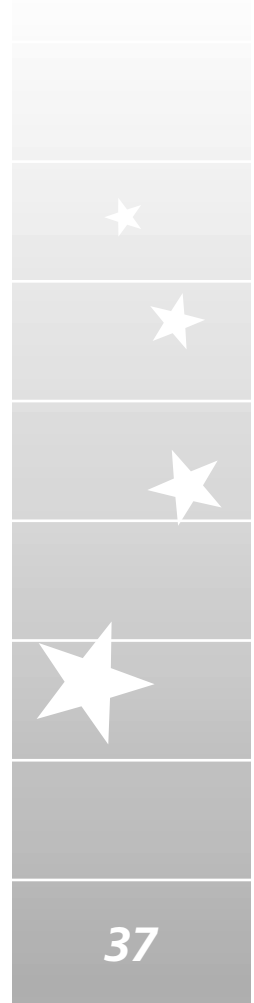
5.2.5 *Non-Coercibility and Verifiability*

Research is needed on methods and protocols to reduce the ability of people to buy or sell votes, or coerce others to vote. One approach that has been discussed is to allow people to vote more than once, with only the last vote counting, thereby preventing potential vote sellers from being able to prove how they vote. Research is needed to determine whether this is practical, particularly when other voting systems (such as poll site paper ballots and absentee ballots) are in use in the same jurisdiction as Internet voting. Research is also needed on the trade-offs between non-coercibility and verifiability. What kinds of voting audit trails can be provided that enable verification of election integrity, but do not permit association of the voter with the vote?

5.2.6 *Economics*

An important factor in determining whether to implement poll site Internet voting systems is their cost relative to other systems, including both paper ballots and DRE systems. It is important to develop an economic model to address this cost-benefit calculation. This should include the costs associated with system acquisition, implementation, technical support, and upgrades for the life cycle of the systems. It is also important to consider whether Internet voting would be a substitute for or an addition to current voting systems for these purposes. Another issue is whether or not public domain computers used for other purposes in schools and libraries can be used for voting. Can they be set-up and maintained in a way that would avoid security risks?

For remote Internet voting, analysis will be needed on the economics of specialized voting devices as well as the cost of providing digital signatures or other appropriate authentication. There also is the related issue of how one pays for digital signatures or biometric authentication. Voters cannot be asked to pay individually because of the prohibition on poll taxes. If election administrators need to pay, it becomes a significant budget expense.



5.2.7 Voter Participation and Access

A key question is how Internet voting would affect turnout, both in general and among different demographic groups (e.g., age, sex, race/ethnicity, income, urban/rural, party affiliation, or occupation). How can this be expected to change as Internet access and use changes among different groups? Research on attitudes towards computers, as well as behavior in related areas, such as making purchases over the Internet, might shed light on attitudes towards Internet voting. Research also needs to be done on how poll site, kiosk, and remote voting affect turnout.

5.2.8 The Election Process

Research is needed on how Internet voting would change the nature of elections and the public's view of elections. Some key topics are:

- How does electronic technology affect people's trust in elections? Does the lack of transparency of automated systems affect public confidence in the process?
- How would Internet voting affect deliberative democracy? Would a result be more initiatives, referenda, and recall votes?
- How can the Internet be used to provide better information about elections? This was viewed as especially important for local elections.
- What effect would Internet voting have on the community ritual aspect of voting? What effect would this have on social capital and civic engagement? What and how relevant is the evidence from states with vote-by-mail?
- How would Internet voting affect all aspects of election administrators' work, in such areas as: voter education, communications with voters, recruitment and training of poll workers, identification and designation of polling places, storage and maintenance of voting equipment, and creation and production of ballots?

5.2.9 Candidates and Campaigns

Research is needed on how Internet voting might change campaigning. How might Internet voting change the premium on candidate characteristics, and the behavior of parties and consultants? How would extended voting periods—a development likely with Internet voting—affect campaigns and fundraising? Should on-screen electioneering be controlled, and if so, how?

5.2.10 Federal, State, and Local Roles

Studies need to be conducted to assess the appropriate authority, responsibility and initiative for each level of government (federal, state, and county) in elections. What is the appropriate role of the federal government in state-administered elections? Is there a need for greater federal involvement in research and election system standards? Is national, rather than state, certification of election systems appropriate, or even constitutional?

5.2.11 Legal Issues

There is a need for research into many legal issues related to Internet voting. Examples include:

- Can laws and international treaties be crafted that would significantly deter fraud and attacks on voting systems?

- Who should be liable for failures of Internet voting systems? Responsibility currently is with election officials, but proprietary computer software may create liabilities that are not under the control of election administrators.
- How would voting-related laws, such as electioneering laws, need to be updated to apply to Internet voting?
- How do e-commerce-related policies and laws, such as those restricting strong encryption or that affect the ability to reverse engineer software, affect Internet voting?

Most of these issues are relevant to poll site Internet voting, but become increasingly important for remote Internet voting.

5.2.12 Registration and Authentication

The workshop identified voter registration as a weak link in current voting systems. There is a need for analysis of how the National Voter Registration Act has affected voter registration, and whether changes are needed. A comparison of state voter registration laws would also be useful. It would be useful to analyze how the Internet could be used to help keep registrations of mobile populations up to date. Several issues related to digital signatures or public key infrastructure need investigation:

- What issues arise related to theft, borrowing, selling, or lending of digital signatures for voting?
- How does one deal with the need to repeatedly upgrade public key infrastructure, as encryption keys necessarily become larger?
- How does one prevent a person from having multiple keys and then voting multiple times?

Research into the potential and practical issues related to biometric authentication for Internet voting would also be valuable. What are the privacy and other policy issues associated with this?

5.3 Research Methods

In addition to the specific research topics identified above, panelists identified some specific research approaches that could be used.

5.3.1 Surveys and Data Analysis

One important line of research would be to use data based on the Census Bureau's Current Population Survey (CPS) and "supplements" on voters and on computer and Internet use. These have large sample sizes and permit analysis of many subsets of the data.

In addition, conventional sample surveys could be used to explore a variety of topics, including public opinion about Internet voting, users' experience with different modes of voting, and election officials' experiences over time with alternative election procedures.

5.3.2 Analysis of Elections and Pilot Projects

It would be useful to analyze other elections that have taken place that may provide insight into Internet voting issues. Some examples of Internet voting have already occurred, including the 2000 Democratic primary in Arizona, the Voting Over the Internet Pilot

sponsored by the Department of Defense's Federal Voter Assistance Project, and poll site demonstrations in several counties around the country. There also have been several uses of Internet or electronic voting in other countries. Experience with private Internet elections, DRE voting systems, early voting, and voting by mail can be examined to study specific issues related to Internet voting. In some cases, it may be possible and desirable to compare counties with Internet voting matched with a similar control country that did not use Internet voting. There is also a need for social science "SWAT" teams that would be able to investigate Internet voting experiments on short notice.

5.3.3 *Experimentation, Modeling, and Simulation of Election Systems*

There is a need to be able to experiment with and simulate elections systems in order to understand and evaluate their technical and social science aspects, and to compare alternative systems. It would be appropriate to establish a center for election experimentation, modeling, and simulation to conduct these activities.

The research issues outlined above are drawn from a very large and diverse research agenda that is both intellectually exciting and highly relevant to important national issues. Many of the technical research topics would advance the state of the art in areas such as security and authentication that are important for electronic commerce and electronic government applications. And many of the social science research issues would contribute to a new understanding of the role of technology and democracy. Internet voting promises significant benefits to democratic processes, but also poses great challenges. This research agenda is essential to address these challenges, and to make sound decisions about the future of election systems in America.

Appendix A: White House Memorandum

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

December 17, 1999

December 17, 1999

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Electronic Government

My Administration has put a wealth of information online. However, when it comes to most Federal services, it can still take a paper form and weeks of processing for something as simple as a change of address.

While Government agencies have created “one-stop-shopping” access to information on their agency web sites, these efforts have not uniformly been as helpful as they could be to the average citizen, who first has to know which agency provides the service he or she needs. There has not been sufficient effort to provide Government information by category of information and service—rather than by agency—in a way that meets people’s needs.

Moreover, as public awareness and Internet usage increase, the demand for online Government interaction and simplified, standardized ways to access Government information and services becomes increasingly important. At the same time, the public must have confidence that their online communications with the Government are secure and their privacy protected.

Therefore, to help our citizens gain one-stop access to existing Government information and services, and to provide better, more efficient, Government services and increased Government accountability to its citizens, I hereby direct the officials in this memorandum, in conjunction with the private sector as appropriate, to take the following actions:

1. The Administrator of General Services, in coordination with the National Partnership for Reinventing Government, the Chief Information Officers’ Council, the Government Information Technology Services Board, and other appropriate agencies shall promote access to Government information organized not by agency, but by the type of service or information that people may be seeking; the data should be identified and organized in a way that makes it easier for the public to find the information it seeks.
2. The heads of executive departments and agencies (agencies) shall, to the maximum extent possible, make available online, by December 2000, the forms needed for the top 500 Government services used by the public. Under the Government Paperwork Elimination Act, where appropriate, by October 2003, transactions with the Federal Government should be available online for online processing of services. To achieve this goal, the Director of the Office of Management and Budget shall oversee agency development of responsible strategies to make transactions available online.
3. The heads of agencies shall promote the use of electronic commerce, where appropriate, for faster, cheaper ordering on Federal procurements that will result in savings to the taxpayer.

4. The heads of agencies shall continue to build good privacy practices into their web sites by posting privacy policies as directed by the Director of the Office of Management and Budget and by adopting and implementing information policies to protect children's information on web sites that are directed at children.
5. The head of each agency shall permit greater access to its officials by creating a public electronic mail address through which citizens can contact the agency with questions, comments, or concerns. The heads of each agency shall also provide disability access on Federal web sites.
6. The Director of the National Science Foundation, working with appropriate Federal agencies, shall conduct a 1-year study examining the feasibility of online voting.
7. The Secretaries of Health and Human Services, Education, Veterans Affairs, and Agriculture, the Commissioner of Social Security, and the Director of the Federal Emergency Management Agency, working closely with other Federal agencies that provide benefit assistance to citizens, shall make a broad range of benefits and services available through private and secure electronic use of the Internet.
8. The Administrator of General Services, in coordination with the Secretary of the Treasury, the Secretary of Commerce, the Government Information Technology Services Board, the National Partnership for Reinventing Government, and other appropriate agencies and organizations, shall assist agencies in the development of private, secure, and effective communication across agencies and with the public, through the use of public key technology. In light of this goal, agencies are encouraged to issue, in coordination with the General Services Administration, a Government-wide minimum of 100,000 digital signature certificates by December 2000.
9. The heads of agencies shall develop a strategy for upgrading their respective agency's capacity for using the Internet to become more open, efficient, and responsive, and to more effectively carry out the agency's mission. At a minimum, this strategy should involve:
 - (a) expanded training of Federal employees, including employees with policy and senior management responsibility;
 - (b) identification and adoption of "best practices" implemented by leading public and private sector organizations;
 - (c) recognition for Federal employees who suggest new and innovative agency applications of the Internet;
 - (d) partnerships with the research community for experimentation with advanced applications; and
 - (e) mechanisms for collecting input from the agency's stakeholders regarding agency use of the Internet.
10. Items 1-8 of this memorandum and my July 1, 1997, and November 30, 1998, memoranda shall be conducted subject to the availability of appropriations and consistent with agencies' priorities and my budget, and to the extent permitted by law.
11. The Vice President shall continue his leadership in coordinating the United States Government's electronic commerce strategy. Further, I direct that the heads of executive departments and agencies report to the Vice President and to me on their progress in meeting the terms of this memorandum, through the Electronic Commerce Working Group in its annual report.

WILLIAM J. CLINTON

###

Appendix B: Workshop Registered Attendees

Kees AartsUniversity of Twente, The Netherlands
Deborah BruntonVoteHere.net
Thomas BryerCouncil for Excellence in Government
Roman BuhlerCommittee on House Administration
Guy DuncanElection Systems & Software
Sean DunneUnited Nations
Jon EisenbergComputer Science & Telecommunications Board
Cheryl A. FainEmbassy of Switzerland
David FruehwaldSoza & Company, Ltd.
Sarah Gilchrist.....Georgetown University
Sharon GilpineBallot.net
Michael GravelPhiladelphia Two Direct Democracy
Marlit HayslettGeorgia Tech
Robert HersheyEngineering and Management Consulting
Philip HowardPew Internet & American Life Project
Christopher K. JonesVirtualWorkroom
Ari JuelsRSA Security Inc.
Kevin J. KennedyWisconsin State Elections Board
Kim KleinBooz • Allen & Hamilton
Helen L. KossMaryland State Board of Elections
Linda H. LamoneMaryland State Board of Elections
Doug LewisThe Election Center
Rebecca MercuriNotable Software, Inc.
Thomas E. MishouOffice of the Georgia Secretary of State
Jeannette Nielsen.....Royal Danish Embassy
Alain PelletierElections Canada
Rene PeraltaYale University
Deborah M. PhillipsThe Voting Integrity Project
Malene PioRoyal Danish Embassy
Priscilla Regan.....George Mason University
Leslie ReynoldsNational Association of Secretaries of State
Dave ScottNational Association of State Election Directors
John SeibelTrueballot, Inc.
Gregory M. ShawUniversity of Pennsylvania
Edgar H. SibleyGeorge Mason University
Richard G. SmolkaElection Administration Reports
J.H. SniderNorthwestern University
Tony Stanco.....FreeDevelopers
Jay StanleyForrester Research
Edward Still.....Lawyers' Committee for Civil Rights Under Law
Mark StramaElection.com
Susan Turnbull.....U.S. General Services Administration
Bara VaidaNational Journal's Technology Daily
Cynthia D. WaddellPSI Net Consulting Solutions
David WeitzelMitretek Systems

Barry WhiteCouncil for Excellence in Government
Dee WhyteImagitas
Natalie WilkisonJapan Economic Review
Lynne WolstenholmeAndersen Consulting
Andrew WynhamSequoia Pacific Voting Equipment
Thom WysongTechno Democracy Project

Appendix C: Glossary

Authentication: The process by which a voter's eligibility to vote is verified; digital signatures are a key component.

Biometric: Any specific and uniquely identifiable physical human characteristic (e.g., retinal map, voiceprint, fingerprint, handwriting) that may be used to validate the identity of an individual.

Client: The device with which voters cast their ballot.

Communications Path: The path between the voting client and the server.

Denial of Service (DOS) Attack: The use of one or more computers to interrupt communications between a client and a server by flooding the target with more requests than it can handle.

Digital Certificate: An electronic credential, issued by a neutral, trusted third party, used to verify the identity of a user. By generating a digital signature, the authenticity and integrity of a document can be verified.

Digital Divide: The gap that exists between various demographic groups in terms of access to computers and information technology.

Digital Signature: A digital code that can be attached to a file that uniquely identifies the sender and the integrity of the file.

Direct Recording Electronic (DRE) System: A voting machine that enters the voter's choices into electronic storage with the use of a touch-screen, push-buttons, or similar device. These votes are stored via a memory cartridge, diskette or smart-card, and added to the choices of all other voters.

Distributed Denial of Service (DDOS) Attack: A more powerful denial of service attack that uses the processing power of multiple computers without the knowledge or consent of their owners to flood and overwhelm the intended target.

Distributed Trust: A voting process model in which authority is distributed among several entities (to guard against insider fraud) such that no single person/entity is responsible for ensuring the integrity of an election.

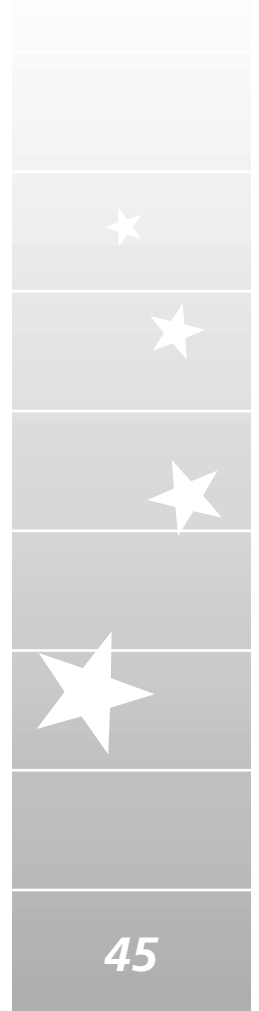
Election Integrity: Ensuring the privacy of a voted ballot, the ability to audit the election for verifiability, and maintaining the security of the system.

Encryption: The transformation of data into a format that cannot be read without the appropriate key; 512-bit is standard for most e-commerce transactions, but election software generally uses 1024-bit.

Encryption Key: A very long number that is used to encrypt and decrypt files.

Federalism: A system of governance adopted by the Framers of the U.S. Constitution that divides power between the state and federal governments.

Internet Service Provider (ISP): A vendor that supplies Internet access.



Interoperability: The ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Kiosk Voting: An intermediate step between poll site and remote voting in which voting terminals would be located outside the polling place but remain under the control of election officials.

Malicious Payload: Software code that is carried by a delivery mechanism, such as a Trojan horse, that is generally intended to do harm to a system.

Platform: The underlying hardware and software of a voting system.

Poll Site Internet Voting: The casting of ballots at public sites where election officials control the voting platform and the physical environment.

Private Elections: Elections conducted by private organizations (e.g., corporations, unions, political parties).

Public Key Infrastructure (PKI): A framework established to issue, maintain, and revoke digital certificates that accommodates a variety of security technologies to ensure authentication, integrity, and confidentiality.

Public Sector Elections: Elections conducted by state officials pursuant to rigid standards and public law.

Reliability: The ability of a system or component to perform its required functions under stated conditions for a specified period of time.

Remote Voting: The casting of ballots at private sites (e.g., home, school, office) where the voter or a third party controls the voting client.

Server: A computer that manages network resources; votes are accumulated and tallied at this location.

Secure Socket Layer (SSL): An encryption protocol used to ensure the authenticity and security of a connection, and the privacy and integrity of a transaction.

Source Code: Software program instructions in their original form; the only format that is readable by humans.

Transparency: The extent to which citizens can meaningfully view and understand how elections are conducted.

Trojan Horse: An apparently harmless program containing hidden code that, once installed, allows for the unauthorized collection, falsification, or destruction of information.

Trusted Authority: A voting model in which a single person/entity is responsible for the tabulation of ballots and the integrity of an election.

Appendix D: Selected References

Articles and Reports

- “A Preliminary Assessment of the Reliability of Existing Voting Equipment.”
The Caltech/MIT Voting Project (February 2001).
- Alvarez, R. Michael, and Jonathan Nagler. “The Likely Consequences of Internet Voting for Political Representation.” (September 2000)
<www.lls.edu/internetvoting/ivote3c.pdf>.
- Benaloh, J., and M. Yung. “Distributing the Power of a Government to Enhance the Privacy of the Voters.” *ACM Symposium on Principles of Distributed Computing* (1986): 52–62.
- California. Office of the Secretary of State. *California Internet Voting Task Force Report*. (January 2000) <www.ss.ca.gov/executive/ivote/>.
- Canada. Elections Canada. *Technology and the Voting Process*. (June 1998)
<www.elections.ca/loi/vot/votingprocess_e.pdf>.
- Canada. Elections Canada. “Technology in the Electoral Process.” *Electoral Insight 2:1* (June 2000) <www.elections.ca/eca/eim/insight0600_e.pdf>.
- Cohen, J. *Improving Privacy in Cryptographic Elections*. Yale University Department of Computer Science Technical Report 372, March 1985
<www.research.microsoft.com/crypto/papers/privel.ps>.
- Cohen, J., and M. Fischer. “A Robust and Verifiable Cryptographically Secure Election Scheme.” *Proceeding of the 26th IEEE Symposium on Foundations of Computer Science* (October 1985): 372–382.
- Craft, Paul. “Internet Voting: Spurring or Corrupting Democracy?” (April 2000)
<paulcraft.net/cfpivote.htm>.
- Cranor, Lorrie Faith. “Voting After Florida: No Easy Answers.” (December 2000)
<www.research.att.com/~lorrie/voting/essay.html>.
- Elliott, David M. “Examining Internet Voting in Washington.” (2000)
<www.electioncenter.org/voting/InetVotingWhitePaper.html>.
- Herschberg, Mark A. “Secure Electronic Voting Using the World Wide Web.” Master’s Thesis, Massachusetts Institute of Technology, June 1997.
- Hoffman, Lance. “Internet Voting: Will It Spur or Corrupt Democracy?” (2000)
<www.netvoting.org/Resources/p219-hoffman.pdf>.
- Jefferson, David, and Deborah M. Phillips. “Is Internet Voting Safe?” (2000)
<www.voting-integrity.org/text/2000/internetsafe.shtml>.
- Jones, Douglas W. “Evaluating Voting Technology.” (January 2001)
<www.cs.uiowa.edu/~jones/voting/uscrc.html>.
- Jones, Douglas W. “E-Voting—Prospects and Problems.” (April 2000)
<www.cs.uiowa.edu/~jones/voting/taubate.html>.
- Mann, Irwin. “Open Voting Systems.” (March 1993)
<www.cpsr.org/conferences/cfp93/mann.html>.
- Neumann, Peter G. “Risks in Computerized Elections.” *Inside Risks*, 5, CACM 33, 11, (November 1990): 170.
- Neumann, Peter G. “Security Criteria for Electronic Voting.” *16th National Computer Security Conference* (September 1993) <www.csl.sri.com/neumann/ncs93.html>.

- Newkirk, M. Glenn. "From Dark Corner to DOT-COM: The Road Ahead for Online Voting." (July 2000) <www.infosentry.com/DarkCorner_to_DOTCOM.htm>.
- Niemi, Valtteri, and Ari Renvall. "How to Prevent Buying of Votes in Computer Elections." *Advances in Cryptology—ASIACRYPT '94*, Vol. 917 of *Lecture Notes in Computer Science*, December 1994, 164–170.
- Nurmi, H., et al. "Secret Ballot Elections in Computer Networks." *Computers & Security*, Vol. 10 (1991): 553–560.
- Peralta, Rene. "Voting Over the Internet." (April 2000)
<www.netvoting.org/Resources/peralta.doc>
- Phillips, Deborah. "Are We Ready for Internet Voting?" (August 1999)
<www.voting-integrity.org/projects/votingtechnology/internetvoting/ivp_title.shtml>.
- Rubin, Avi. "Security Considerations for Remote Electronic Voting over the Internet." (November 2000) <avirubin.com/e-voting.security.html>.
- Sako, Kazue and Joe Killian. "Receipt-Free Mix-Type Voting Scheme: A Practical Solution to the Implementation of a Voting Booth." *Advances in Cryptology—EUROCRYPT '95*, Vol. 921 of *Lecture Notes in Computer Science*, May 1995: 393–403.
- Salomaa, A. *Public-Key Cryptography*. Springer-Verlag, 1990.
- Saltman, Roy G. "Accuracy, Integrity, and Security in Computerized Vote-Tallying." U.S. Department of Commerce, National Bureau of Standards, Special Publication 500–158, August 1988.
- Saltman, Roy G. "Assuring Accuracy, Integrity and Security in National Elections: The Role of the U.S. Congress." (February 1993)
<www.cpsr.org/conferences/cfp93/saltman.html>.
- Saltman, Roy G. "Computerized Voting." Chapter 5 in *Advances in Computers*. Vol. 32, Academic Press, 1991: 255–305.
- Saltman, Roy G. "Effective Use of Computer Technology in Vote-Tallying." U.S. Department of Commerce, National Bureau of Standards, Report 75-685, March 1975 (reprinted as NBS SP500-30, April 1978).
- Schneier, Bruce. *Applied Cryptography*. John Wiley & Sons, New York, 1994.
- Schoenmakers, Berry. "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting." *Advances in Cryptology—CRYPTO '99*, Vol. 1666 of *Lecture Notes in Computer Science* (1999): 148–164.
- Schoenmakers, Berry. "Compensating for a Lack of Transparency."
<www.netvoting.org/Resources/p231-schoenmakers.pdf>.
- Shamos, Michael Ian. "Electronic Voting—Evaluating the Threat." (March 1993)
<www.cpsr.org/conferences/cfp93/shamos.html>.
- Stanton, Michael. "The Importance of Recounting Votes." (November 2000)
<www.notablessoftware.com/Press/electronic_voting_in_brasil.htm>.
- Traugott, Michael W. "Why Electoral Reform has Failed: If You Build It, Will They Come?" (October 2000) <www.netvoting.org/Resources/traugott.doc>.
- Traugott, Michael W., and Robert G. Mason. *Preliminary Report on the Characteristics of the Oregon Electorate Participating in the Special General Election for the U.S. Senate on January 30, 1996*. (May 1996)
<www.netvoting.org/Resources/traugott2.doc>.

Waddell, Cynthia. "The Growing Digital Divide in Access for People with Disabilities: Overcoming Barriers to Participation in the Digital Economy." (May 1999)
<www.icdri.org/the_digital_divide.htm>.

Waskell, Eva. "Overview of Computers and Elections." (March 1993)
<www.cpsr.org/conferences/cfp93/waskell.html>.

Miscellaneous

The Future of Internet Voting. A Symposium Co-Sponsored by The Brookings Institution and Cisco Systems, Inc. (January 20, 2000)
<www.brookings.org/comm/transcripts/20000120.htm>.

Jefferson, David. *Internet Voting.* Powerpoint presentation. (August 2000)
<www.netvoting.org/Resources/InternetVoting-FEC.ppt>.

Strassman, Marc. *Toward a Ubiquitous E-Democracy Powered by a Universal PKI.*
<bookchat.org/PKIForum.ram>.



Acknowledgments

The Internet Policy Institute (IPI) would like to thank all of the individuals and organizations that made this report possible. Special thanks go to C.D. Mote Jr., who chaired the workshop and the project's executive committee, David Cheney, the principal investigator of the project, and Richard Schum, who served as project director. Erich Bloch, chairman of IPI Research Advisory Board, and Gerry Glaser of IPI also provided critical advice throughout. The project benefited greatly from the extensive advice and guidance from members of the executive committee, which spent many hours helping to shape the workshop and reviewing the many iterations of the report. The project also relied upon the previous work of the California Task Force on Internet Voting and David Jefferson, whose counsel and expertise were invaluable in drafting the report.

IPI would also like to thank the panelists at the workshop, who were critical to the project's success. They contributed a great wealth and breadth of expertise, provided additional materials, and commented on an early draft the report. Observers at the workshop also contributed additional views and information.

We extend a special note of appreciation to IPI board member Adam Powell and Euraine Brooks of the Freedom Forum, whose work in hosting the workshop contributed greatly to its success. Thanks also goes to Amy Friedlander and the Integrated Communications Team at SAIC for providing assistance in editing and production of the report.

Finally, we would like to thank the National Science Foundation for its support of the project, and especially Larry Brandt and Valerie Gregg for their guidance throughout the project.

IPI Board of Directors

James L. Barksdale, (IPI Chairman), Partner, The Barksdale Group

G. Wayne Clough, (IPI Chairman), President, Georgia Institute of Technology

Erich Bloch, President, The Washington Advisory Group

Antoinette Cook Bush (Toni), Executive Vice President, BroadwaveUSA/Northpoint Technology Ltd.

Thomas Casey, Vice Chairman and CEO, Global Crossing Ltd.

Vinton G. Cerf, Senior Vice President of Internet Architecture & Technology, WorldCom

James W. Cicconi, General Counsel & Executive Vice-President, Law & Government Affairs, AT&T Corporation

Michael A. Daniels, Senior Vice President and Sector Manager, Technology Applications Sector, Science Applications International Corporation (SAIC)

Francis A. "Fran" Dramis, Executive Vice President, CIO and eCommerce Officer, BellSouth Corporation

Esther Dyson, Chairman, EDventure Holdings Inc.

Sherrilynne Fuller*, Head, Division of Biomedical and Health Informatics, School of Medicine, University of Washington

Newt Gingrich*, CEO, The Gingrich Group

Robert Herbold, Executive Vice President and Chief Operating Officer, Microsoft Corp.

Christine Hughes, Chairman, Highway 1

Robert O. McClintock, Co-Director, The Institute for Learning Technologies at Teacher's College, Columbia University

Kimberly Jenkins, President, Internet Policy Institute

Robert E. Kahn*, President and CEO, the Corporation for National Research Initiatives

Roberta Katz*, CEO, Article III, Inc.

Ira C. Magaziner*, President, SJS Advisors, Inc.

Mary Meeker, Managing Director, Morgan Stanley Dean Witter

Harris N. Miller, President, Information Technology Association of America (ITAA)

Mario Morino, Chairman, Morino Institute and Special Partner, General Atlantic Partners

Adam Clayton Powell III, Vice President, Technology and Programs, The Freedom Forum

Hal Varian, Professor and Dean, School of Information Management, University of California at Berkeley

George Vradenburg, Senior Vice President for Global and Strategic Policy, America Online Time Warner, Inc.

** Board member emeritus*

IPI Research Advisory Board

The Internet Policy Institute Research Advisory Board provides advice on the overall direction and priorities of the IPI's research program; aids in identifying and recruiting scholars; and reviews and ensures the quality and balance of IPI research products. The members are:

Erich Bloch (Chair), President, Washington Advisory Group

Daniel E. Atkins, Professor of Information and Professor of Electrical Engineering and Computer Science at the University of Michigan.

Jane Fountain, Associate Professor of Public Policy, John F. Kennedy School of Government, Harvard University.

Francis Fukuyama, Professor of Public Policy and director of the International Commerce and Policy Program, George Mason University.

B. Keith Fulton, Executive Director of Corporate Outreach, America Online

Donna Hoffman, Associate Professor of Management, Owen Graduate School of Management, Vanderbilt University.

Deborah G. Johnson, Professor and Director of the Program in Philosophy, Science and Technology, School of Public Policy, Georgia Institute of Technology

Brian Kahin, Director of Center for Information Policy, and Visiting Professor in the College of Information Studies, University of Maryland.

Rob Kling, Professor of Information Science and Information Systems, Indiana University–Bloomington, and Director, Center for Social Informatics

Theodore O. Poehler, Vice Provost for Research, and Research Professor of Materials Science and Engineering, The Johns Hopkins University

Jorge Reina Schement, Professor of Telecommunications and Co-Director of the Institute for Information Policy, Pennsylvania State University.

Larry Smarr, Strategic Advisor, School of Engineering, University of California at San Diego.

Hal R. Varian, Dean of the School of Information Management and Systems at UC Berkeley, with joint appointments in the Haas School of Business and the Department of Economics.

Ernest James Wilson, Director, Center for International Development and Conflict Management, and Associate Professor of Government and Politics and Afro-American Studies and a Faculty Associate in the School of Public Affairs, University of Maryland.

