PUBLICATION

Digital Democracy: Voting in the Information Age

Joseph Butcher, David Sulek, Erin MacDougall, Katie Hines, Anna Kertesz, and David Svec

October 2002

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

A Booz Allen Hamilton Study

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-83-6 **P-02-7**

All of the authors work at Booz Allen Hamilton. David Sulek (Principal Investigator) is a Senior Associate specializing in analysis of national security, homeland security, and public-private partnership policy issues. Joseph Butcher (Principal Investigator) is an Associate specializing in telecommunications and Internet policy and security analysis. Erin MacDougall is an Associate specializing in policy analysis in the areas of homeland security, information assurance, and Internet Voting/Election Reform. David Svec is an Associate specializing information security and privacy issues. Kathryne Hines is a Senior Consultant specializing in policy research and analysis in the areas of information security and Internet Voting/Election Reform. Anna Kertesz is a Senior Associate specializing in the legal and policy issues associated with privacy on the Internet.

October 2002

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz Allen Hamilton
Center for Excellence in Education
Commission of the European Communities
Critical Path
CyraCom International
Ellacoya Networks, Inc.
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
Hitachi Research Institute (Japan)
IBM Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis–Nexis
John and Mary R. Markle Foundation
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
PDS Consulting
PetaData Holdings, Inc.
Samara Associates
Skadden, Arps, Slate, Meagher & Flom LLP
Sonexis
Strategy Assistance Services
TOR LLC
United States Government:
- Department of Commerce
  - National Telecommunications and Information Administration
- Department of Defense
  - National Defense University
- Department of Health and Human Services
  - National Library of Medicine
- Department of the Treasury
  - Office of the Comptroller of the Currency
- Federal Communications Commission
- National Security Agency
- United States Postal Service

Upoc
Verizon

Contents

Illustrations

Tables

Figures

Acknowledgements

The authors gratefully acknowledge the following people who reviewed and commented critically on the draft version of this report. Without their consideration, input, and encouragement, this study could not have been completed:

David M. Anderson
Victor Babbitt
Anthony T. Green
Michael Griesdorf
Carla Johnston
Howard Kaye, Jr.
William C. Kimberling
Herbert E. Marks
Vincent Mosco
Peter G..Neumann
Andrea Ricci
Julie Ryan
Peter Shapiro
Brian Stewart
John Woodward

These reviewers and the Program's Affiliates, however, are not responsible for or necessarily in agreement with the views expressed here, nor should they be blamed for any errors of fact or interpretation.

The authors gratefully acknowledge the insights and contributions of many individuals without whom this paper could not have been published. First and foremost, several of our professional colleagues contributed invaluable research and analysis during the course of our study. Those individuals include Lori Cloutier (Election Reform legislative initiatives), Derek Dickey (the history of referendums and initiatives, the Australian ballot), Heather Dobbins (privacy and digital signature legislation), Kimberley Klein (the "business" of Internet voting), James Kliner (the history of voting), and Sharon Russ (international Internet voting initiatives). The authors also wish to acknowledge the insightful counsel of several senior Booz Allen leaders who supported us throughout the course of this study, including: Thomas Fuhrman, Michael Delurey, Richard Wilhelm, Christopher Kelly, and Mike McConnell.

The authors also extend their thanks and appreciation to the staff and affiliates of the Harvard University Program for Information Resources Policy. In particular, we benefited greatly from the insights, guidance, and patience of Dr. Oettinger and John LeGates, the editing and of Ellin Sarot, and the tremendous assistance of Mary Walsh throughout this process.

Executive Summary

On Election Night in November 2000, the Nation was spellbound by one of the most intriguing electoral chapters in the history of the republic. That election—and the controversial events that followed for days and weeks in Florida—offered riveting political theater, shedding light on a normally transparent electoral process and exposing serious flaws. Shortcomings included poorly designed ballots, antiquated voting machines, inadequately trained poll workers, and disparate types of voting equipment that varied widely by precinct. In the wake of electoral turmoil, lawmakers and elected officials faced the challenge of how best to reform the electoral system. Complicating those efforts were the competing interests and roles of federal, state, and local jurisdictions and the high costs associated with acquiring new voting equipment and training poll workers.

Immersed within this debate is the complex issue of using advanced technologies, and specifically the Internet and its applications, as an alternative to the traditional polling booth. Even before the problems of the electoral system manifested in such a public fashion, experiments with a new form of voting—*Internet voting*—were underway. Wired citizens pressed for consideration of Internet voting, and election officials and legislators at first appeared eager to please constituents. But lingering questions remained. Specifically, considering Internet voting as an alternative to traditional forms of casting ballots raised five broad issues:

- Access—equal access to the ballot is critical in our democracy. Events in Florida , and other states such as New Jersey and Missouri, revealed how real or perceived disparities in access create questions about the legitimacy of an election. It is important that "digital ballot boxes" do not exacerbate the perceived *digital divide* and result in the cyberspace "haves" disproportionately influencing the outcome of an election.

- Security—integrity of an election is paramount in a democratic society. Actual—or perceived—manipulation of votes or election results can erode the public's confidence. Security risks are probably the most discussed issue associated with Internet voting, and for good reason. Moving ballots into the digital realm introduces a whole new series of threats to our electoral system, and building highly secure, trustworthy systems is a prerequisite to the widespread adoption of Internet voting solutions.

- Privacy—the secrecy of the ballot is a vital component to a free and fair election. When a vote is held secret, it is difficult for voters to be strong-armed or coerced, and they are free to vote their conscience without disclosure. The Internet's ubiquity raises legitimate concerns about how the information contained in digital ballots will be protected in transmission across the Internet and when stored in electoral databases.

- Technology—developing technologies to improve the speed and accuracy of voting remains a cornerstone of our electoral process. Automation has greatly improved the ability of election officials to more quickly and accurately count and recount votes. That statement might, on the surface, belie the events in Florida. However, the reality is a few counties in Florida with old technologies were responsible for protracted recounts of the dreaded "hanging chad." There are significant technological issues—particularly scalability and overall Internet reliability—that are key to the widespread use of Internet voting solutions.

- Civic Participation—our representative democracy is based on the power of individual citizens to participate in their governance by voting. The Internet may empower citizens by offering increasingly direct access to elected representatives and to new channels of action, such as on-line poling and mass e-mails, to satisfy political objectives. The chief issue is whether these developments naturally encourage the United States to transition toward a more direct, possibly reactive form of democracy.

Each issue is important in its own right, but there are four practical considerations key to forging a path toward digital democracy. First, it is important that policy makers, legislators, technologists, and others consider Internet voting holistically. Alongside technical issues of Internet security, reliability, and scale are equally complex issues related to American voting customs, electoral procedures, election law, budgetary constraints, questions of fairness, and federalism. Second, it is important to distinguish between Internet voting and election reform. While the events in Florida captured the attention of the general public, the push for Internet voting began more than a year before the "butterfly ballot" and "hanging chad." Internet voting raises issues related to, but not directly synonymous with, those in election reform. Third, each of the five issues identified in this study needs to be examined in light of electoral tensions the framers of the U.S. Constitution and later thinkers tried to balance, many of which are applicable today. Fourth, the problems encountered during the election of 2000 coupled with increased interest in and experimentation with Internet voting may yield constructive results. The revelations of the flaws in the established electoral system may reduce resistance to change and promote a careful, deliberate, and thoughtful use of Internet technologies that may, in the end, build a sense of trust and acceptance among the electorate.

Chapter One

Introduction

Election year 2000 was marked in the United States by competitive races for presidential nominations in both major political parties and ended with one of the most controversial chapters in the country's electoral history. While the presidential candidates, George W. Bush (Republican) and Albert A. Gore, Jr. (Democrat), their legal teams, Florida election officials and jurists, and the U.S. Supreme Court justices all jockeyed for center stage, the electoral system of United States itself provided the turbulent backdrop. Poorly designed ballots confused voters. Voting machines proved inaccurate. Premature and incorrect media projections on election night all frustrated both candidates and the public. In the aftermath, challenges to the veracity of the outcome were mounted in several states, notably Florida and New Mexico.

Even before such problems of the electoral system became front-page news, federal, state, and local governments had begun to examine and experiment with a new method of voting, Internet voting. Increasing general acceptance of Internet technologies and applications, such as on-line banking and electronic commerce (e-commerce), had already fostered a growing interest in the possibility of Internet voting. Wired citizens, empowered by the feature-rich and information-laden Internet, provided a foundation for the consideration of Internet voting as an alternative to the traditional polling booth. To meet perceived opportunities in a new market, a host of dot-com companies specializing in Internet voting technologies emerged on the scene. Election officials and legislators appeared eager to please their constituents and began to study the Internet as part of an effort to modernize the U.S. election infrastructure.

Those same public officials, bolstered by concerns voiced by Internet policy and security experts, shared legitimate and far-reaching concerns about Internet voting, including the following: Will all U.S. citizens have equal access to voting? Are citizens aware of and willing to accept risks that may be introduced with Internet voting, risks such as potential new forms of fraud and abuse, in exchange for convenience? Will digital ballots be secret? Is the Internet sufficiently reliable and robust to support Internet voting in national elections? Can Internet voting fundamentally transform how citizens participate in their democracy?

1.1 Background and Purpose of This Study

This study was launched as a joint project of the Booz Allen Hamilton and the Harvard University Program for Information Resources Policy to explore the policy and technology issues raised by growing public interest in "digital democracy."[1] The purpose of this study is to frame

[1]For the purposes of this report, "digital democracy" is defined as the exchange of ideas and opinions as part of the democratic process by means of the Internet.

the policy and technology issues associated with the prospect of Internet voting. The intent is not to adopt a formal position on the merits of Internet voting but, rather, to offer an even-handed account analysis of the issues, with the following goals:

- to develop intellectual capital to inform and shape the discussions of digital democracy topics by policymakers, technologists, and academics;
- to frame the issues involved in digital democracy in a similarly even-handed manner; and
- to explore this emerging possibility of Internet voting in the within the context of digital democracy, which is closely linked with public and private concerns about security and privacy.

As the focus of the study became clearer, Internet voting became the primary topic, for three reasons. First, in 1999 on-line voting technologies had emerged as a new market for dot-com start-ups. Specifically, several dot-com vendors, such as VoteHere.net and election.com, began to market Internet-based voting solutions to state and local governments, high schools and universities, and labor unions. Second, interest had grown at the federal and state levels in using on-line applications to create new efficiencies and services, and the increasing acceptance and availability of on-line government services had generated interest in other applications and uses, such as voter registration and voting. Third, the prospect of using the Internet in elections had begun to raise important questions about security, privacy, and the reliability of the Internet.

1.2 Organization

Following this introduction, **Chapter Two** examines ways in which Internet voting has surfaced in several debates on democracy in the "information age." **Chapter Three** outlines issues related to access, specifically how Internet voting may exacerbate what has come to be called "the digital divide." **Chapter Four** explores the issues of security raised by Internet voting, including risks to the integrity of an election posed by Internet viruses, worms, and other "cyber" threats. **Chapter Five** considers privacy issues that arise with Internet voting, notably the difficulty of protecting the secrecy of ballots. **Chapter Six** describes several technological issues involved in Internet voting, from concern about the reliability of the Internet to problems of human-machine interfaces. **Chapter Seven** discusses ways in which Internet voting may affect or be affected by increasing civic participation over the Internet. The report concludes in **Chapter Eight** with some thoughts on how technological innovations may influence the way in which U.S. citizens may elect political leaders in the future—that is, the prospect of a digital democracy.

Three appendices follow the body of the report. **Appendix A** presents information on the U.S. electoral system, describes the procedures and processes of the conduct of elections, and provides a historical basis for the discussion of how the Internet may transform U.S. voting. **Appendix B** recounts several trials and experiments with Internet voting in the United States since 1999. **Appendix C** briefly discusses other studies of Internet voting and describes other forms of on-line voting, such as proxy voting and international applications of Internet voting.

Chapter Two

What Is Internet Voting?

Considering the sanctity of the ballot box, John Quincy Adams once remarked, "Always vote for principle and, though you may vote alone, you may cherish the sweetest reflection that your vote is never lost." This sentiment is as applicable today as it was in the nineteenth century. Democracy in the United States is based on the power of citizens to exercise the right to vote their conscience and to do so without interference, coercion, or fear of tampering with their vote. Any breach of confidence in the electoral process can erode the public trust in government.

Technology has been key to ensuring that votes are counted and "never lost." As early as 450 B.C., the Athenians used "counting machines" to cast votes for magistrates and other elected officials and to prevent tampering and coercion.[1] In the United States, pull-lever machines were first introduced in New York State in 1892 to prevent the stuffing of ballot boxes, which was commonplace during the reign of Tammany Hall in the 1880s. The use of punch cards emerged in the United States in the 1960s, as a type of ballot that eased the process of tallying the vote. A decade later, direct recording equipment and optical scanners came into use for the casting and counting of ballots. Also in the 1970s election officials began to employ software programs to speed tallying and improve the accuracy of the counting, recounting, and reconciliation of ballots. Given the history of technological innovations in elections, the question naturally arises: Why not vote over the Internet?

This chapter opens with a summary description of some key foundations of elections and then looks at the emergence of the digital democracy and Internet voting as policy issues. It identifies several broad issues related to the prospect of Internet voting, issues individually explored in later chapters.

2.1 Foundations of Voting and Elections

Three foundations of voting and elections are noted here. First is the relationship of democracy, voting, and elections. In a democracy, power is vested in the citizens through the franchise. Voting is an individual act that reflects a voter's preferences. Elections are the means

---

[1]The Athenians used a variety of methods, notably voting by lot, to elect public officials: pebbles, pottery shards, olive leaves, and bronze discs were used as lots to express preferences. The most interesting Athenian innovation may have been the *cleroterian*, or allotment machine, wood machines placed in public venues to collect citizens' votes. The machines are early forms of the "ballot box" or "election machine." Athenians were provided, for example, with two pebbles, one black, one white, with each color representing a candidate. Citizen inserted a pebble representing the voting preference into one slot and placed the second one into a discard slot. The machine provided voters with anonymity and prevented tampering by allowing election officials to reconcile the total number of black and white pebbles to ensure a fair vote. See E. S. Staveley, *Greek and Roman Voting and Elections* (Ithaca: Cornell University Press, 1972), 62-63, 115.

by which citizens express a collective power and will.[2] At the heart of the democratic ideal is the notion that citizens vote their consciences freely, without fear of government reprisal or coercion. Any breach of confidence in the integrity and legitimacy of elections threatens the public trust.

Second, despite the tremendous political, social, cultural, economic, and technological changes that have occurred since elections in Ancient Greece through to the recent presidential election in the information age, several elements have remained constant. Specifically, six elements basic to elections are constant through all historical eras: the voter, the candidate, political discourse, a ballot, the tally, and a herald (see **Table 2-1**).

Third, the term "electoral process" is often invoked here. This term encompasses the life cycle of an election, from voter registration, which usually occurs months before an election, to the archiving of results after an election (see **Table 2-2**). Although ordinarily citizens think of elections as occurring only once a year, election officials need to complete many activities that go on year round in order to prepare for, conduct, and manage an election (see **Appendix A**).

2.2 Digital Democracy

The information age, typified by the Internet and its apparently ubiquitous accessibility, has begun to transform many cherished democratic traditions and practices. The concept of a *digital democracy*—the exchange of ideas and opinions as part of the democratic process conducted over the Internet—is based on the notion that the Internet has changed the way citizens interact with one another and with their elected representatives. The Internet is has already influenced democratic processes as well as a wide range of stakeholders (see **Table 2-3**).

Both major political parties in the United States and their candidates have increasingly turned to the Internet to promulgate political positions, customize campaign messages, raise funds, and mobilize campaign volunteers. During the 2000 presidential primary season, the major candidates sponsored official "for-president" Web sites on the Internet that provided information on their positions, informed prospective volunteers across the country, and served as a fundraising instrument. Public interest groups, grassroots movements, and other political organizations are using the Internet to eliminate traditional barriers to organizing groups around a cause, such as cost or geography.[3] People use the Internet to gather information on candidates and issues, use

---

[2]Elections and voting are not, however, the province exclusively of democracy. Elections are also held in countries and by organizations that are not democratic. The College of Cardinals, for example, elects the popes by secret ballot, in a process conducted among only Cardinals of the Church, not by all Catholics.

[3]The protests against the World Trade Organization, the International Monetary Fund, and the World Bank in 1999, in Seattle, Washington, and Washington, D.C., showed that even loosely affiliated civic or grassroots organizations can use the Internet to post information, mobilize people, and coordinate activities.

Internet chat rooms express their views, engage in political discussion with elected representatives, and thereby participate in the political process in innovative ways.[4]

Table 2-1

Basic Elements of Elections

Element	Description	Origin
Voter	A voter is defined by the franchise, by which a nation or other authority grants an individual the right to vote, and by citizenship, which confers civic privileges and responsibilities from which the right to vote is historically derived.	The city-state of Athens in 451 B.C. determined that men of an appropriate age and ancestral heritage (both parents of Athenian citizenship) were eligible to participate in politics.
Candidate	In elections, voters select leaders and public officials from a pool of candidates.	From *candidatus*, the Latin for an office seeker "in white," referring to the white togas candidates in ancient Rome wore.
Public Discourse	Spoken or written, public discourse is vital to elections. The merits of an issue or candidate often are publicly discussed in an open forum before putting them to a vote.	In ancient Athens, citizens over the age of 18 could engage in political discourse on matters before the Assembly.
Ballot	Ballots provide citizens with a mechanism by which to cast votes in an election, often in a manner that protects the identity of the voter and separates it from the vote cast.	From the act of voting by "lot," used by the Athenians for a variety of public votes, including election of public officials, the rendering of verdicts in trials, and votes for ostracism.
Tally	The recording of votes, or tally, is critical to any election. Inaccurate or fraudulent tallies can lead to questioning the integrity of an election.	The first systematic process for counting votes was developed by the ancient Romans, whose election officials and magistrates "tabulated" individual votes on wax tablets.
Herald	The final step in an election is heralding or disseminating the results to the general public.	In the Greek system, a herald announced the results of a vote to those outside the Assembly.

Source: Booz Allen Hamilton.

The explosive growth in diverse uses of the Internet coupled with its penetration into daily life, has sparked public interest in on-line voting. With people generally able to use the Internet to shop and pay bills on-line and file electronic federal and state tax returns, the logical next step appears to be casting votes on line. Internet voting could offer citizens the opportunity to vote from home on Election Day, instead of queuing up at local precincts. It could ease access to the ballot box for disabled voters. It could allow states and localities to count absentee ballots in real time. Yet voting over the Internet also gives rise to serious questions about how on-line voting might fundamentally transform citizens' interactions with elected representatives and to concerns about Internet access, security, reliability, and privacy.

[4]In addition to using Internet chat rooms and official candidate sites, in the United States people are increasingly active politically on the Web. In 1999-2000, Web sites for the Democratic and Republican presidential candidates proliferated in support of them (or opposing their positions and voting records). One such site was Netizens for Bradley (no longer available), which offered the candidate's views on major issues.

Table 2-2

The Electoral Process

Pre-Election	Election	Post-Election
• Party and candidate registration • Nomination planning and implementation • Voter registration • Voter education • Election materials and equipment – Strategic planning – Procurement – Testing • Distribution of absentee ballots • Recruiting and training of staff • Customer service activities	• Distribution of materials • Preparation of the site • Deployment and training of staff • Customer service activities • Casting of votes • Processing and tabulation of votes	• Recovery and evaluation of materials and equipment • Re-tabulation of votes • Auditing of election process • Certification of election results • Communication of results • Archival activities
▲	▲	▲
Preparation for an election occurs over the longest period of the cycle. Voter registration is the main task in this period, along with campaigns to "get out the vote" and the creation and design of the ballot.	The election spans the time when voters can cast votes, both absentee and in-person. Most work in this period occurs on a single resource-intensive day. The processing and tabulation of votes also occur on this day.	The period when auditing and recounts take place, materials and equipment are recovered, and election results are certified and communicated to the public.

Source: Booz Allen Hamilton.

2.3 Internet Voting

Six factors contributed to attracting the attention of the media, government election officials, elected representatives, office seekers, think tanks, dot-com vendors, and the public at large to Internet voting (see **Table 2-3**). Some of these factors may have helped spawn the first Internet-based binding election, the Arizona Democratic presidential primary in March of 2000. In the primary, registered Democrats were given the opportunity to cast votes over the Internet. Of the approximately one hundred thousand who voted, nearly 40 percent accessed a voting site on the Internet, entered a personal identification number (PIN), and cast a binding vote.[5] This was a remarkable event, not only for its historical significance but also because as recently as early

[5]James Ledbetter, "Arizona Democrats, Online Voting," *The Industry Standard Magazine* (March 10, 2000), [On-line]. URL: http://www.thestandard.com/article/0,1902,12858,00.html (Accessed April 24, 2001.)

Table 2-3

Digital Democracy and the Internet

Campaigns	Elections
The Internet offers an inexpensive, distributed venue for raising funds, mobilizing volunteers, and communicating positions on issues.	The Internet eases access to the voting process and has renewed interest in the electoral process, particularly for the technology-savvy "Gen X" community.
Citizens	**Grassroots**
The Internet provides direct access to information and empowers citizens by creating new "networks" and organizations.	The Internet removes traditional geographic and financial barriers for grassroots and civic organizations.
Politicians	**Governments**
The Internet provides politicians with a means to reach out to constituents on issues and to "take the pulse" of the electorate.	The Internet creates opportunities for government to allow citizens to participate in governance increasingly directly through electronic town halls and "wired" legislative bodies.

Source: Booz Allen Hamilton.

1999 none of the fifty states had even seriously contemplated Internet voting.[6] Dot-com vendors of on-line voting technologies and other proponents of Internet voting hailed the Arizona primary as a watershed and as evidence that voting was preparing to enter the twenty first century at "Internet speed." Opponents countered that the use of Internet technology for voting was premature and exposed voters in Arizona to fraud, abuse, and security vulnerabilities.[7]

Voting over the Internet consists of more than logging on to a Web site and casting a vote that is then transmitted over the Internet. Internet voting, as the term is used here, means a form of voting in which voters register to vote and request, receive, complete, and submit a ballot all on the Internet. In defining Internet voting, and for an analysis of the issues involved in it, three distinctions are important:

---

[6]Late in 1998 and early in 1999, California considered the possibility of Internet voting, but critics voiced concern about the security of the Internet. As a result, "the California Internet Voting Task Force was convened by Secretary of State Bill Jones to study the feasibility of using the Internet to conduct elections in California. More than two dozen experts in the field of data security, elections and voter participation were asked to volunteer their time and expertise in the development of [a] report." For the report (published Jan. 18, 2000), see URL: http://www.ss.ca.gov/executive/ivote/ (Accessed May 2, 2001.)

[7]For example, in 2000 the Voting Integrity Project filed suit claiming that, under the Voters' Rights Act of 1965, electronic voting systems violated the rights of minority groups (see section 2.3.3). For the legal claim and related press releases, see URL: http://www.voting-integrity.org/ For an analysis of the Arizona primary, including a description of the VIP's objectives, see "No Voting Opportunity for All," *Wired* Magazine (March 13, 2000), [On-line]. URL: http://www.wired.com/news/politics/0,1283,34914-2,00.html (Accessed Aug. 18, 2001.)

Table 2-4

Drivers of Internet Voting

Catalyst	Description
Electronic commerce	The growth and acceptance of the Internet have fueled interest in Internet voting. As of early 2001, more than 92 million North Americans use the Internet, an increase of 50 percent from 1999. As voters become more accustomed to on-line transactions, the level of acceptance, confidence, and trust will grow.
Electronic government	Parallel to the development of e-commerce are e-gov initiatives. Filing electronic tax returns and obtaining government forms and information from government Web sites increase citizens' interest in and use of the Internet to access government institutions.
A "digital democracy"	The Internet increases the volume of information available to citizens, facilitates interaction with elected representatives, encourages direct participation in politics, and removes traditional barriers to populist movements. A growing sense of "on-line empowerment" has begun to spill over into traditional channels of political action, such as political campaigns.
2000 presidential campaign	Major presidential candidates sponsored official "for-president" Web sites, to put forward information about the candidates for potential voters and to pull data to use to hone campaign messages. The role of the Internet in fundraising may be the most far-reaching legacy of the 2000 campaign. Several candidates, notably John McCain (Rep.-Ariz.), used Web sites to receive campaign contributions.
Voter access	The desire to offer on-line voting capabilities is in concert with other efforts to increase voter access and turnout. Many initiatives, such as Vote By Mail in Oregon, for example, were designed to facilitate voter registration and voting. Internet voting appears to be the next logical step to ease voting processes and procedures and enhance access for all potential voters.
Dot-com marketplace	Dot-com startups, venture capitalists, and leading hardware and software companies, such as Cisco, Verizon, and EDS, regard Internet voting as an emerging, hot "Internet" market. Since 1998, more than half a dozen dot-coms have gained media attention for conducting actual or trial on-line elections. Two of the largest—VoteHere.net and election.com—received more than $10 million in venture capital and began to market potential customers at the federal, state, and local levels.

Source: Booz Allen Hamilton.

- **Internet registration vs. Internet voting.** Although discussions of Internet voting often center on the submission of electronic ballots—that is, on the issues of the security, integrity, and privacy of ballots—the Internet may nevertheless come to play a role in facilitating on-line voter registration.
- **Poll-site vs. remote voting.** Such discussions often involve a comparison of poll-site voting (i.e., using Internet connections and kiosks at traditional polling sites) and remote voting (i.e., using Internet connections, software, and hardware to allow voters to vote from a location, such as home or office, other than an official polling site).[8]
- **Internet voting vs. electronic voting.** Although the Internet introduces a new technology that may make voter registration and voting more efficient and may allow results to be available more quickly than at present, it would not be the first use of electronic hardware and software in the electoral process. Many voting machines already

[8]For a discussion of proposed types of Internet voting, see the California Internet Voting: A Report on the Feasibility of Internet Voting. See also Deborah M. Phillips and David Jefferson, "Is Internet Voting Safe?" Voting Integrity Project (July 10, 2000), [On-line]. URL: http://www.voting-integrity.org/text/2000/internetsafe.shtml (Accessed April 18, 2000.)

use software to collect, record, and count votes, and in some states and localities voters can vote by telephone or facsimile (fax).[9]

2.4 The Issues

The allure of Internet voting has generated a discussion that centers on five broad issues that may affect the viability of Internet voting in the next five to ten years: access, security, civic, security, privacy, technology, and civic participation. These issues, sketched in this chapter, are discussed individually and in detail in subsequent chapters.

Access. Ensuring universal and equal access to the ballot is critical to democracy in the United States. In 1999, officials in the Clinton administration, members of Congress, leaders in industry, and academics all began to analyze the disparity in cyberspace known as the *digital divide*.[10] This disparity, real or perceived, leads to the view that offering government and other public services over the Internet favors those with the means to acquire computer equipment and, therefore, access to the Internet. For Internet voting, this could prove a significant problem at the state and local levels, where government is responsible for providing equal access to the ballot box. Equal access to the ballot box arose as a major issue during the national election of 2000, most visibly in Florida but also in other states, such as New Jersey, where poor and minority communities use old equipment to vote.[11] In light of these concerns, would Internet voting inherently favor the cyberspace "haves" by offering them greater access to the ballot box than the "have nots" and, as a result, disproportionately give them greater influence on the outcome of an election?

---

[9]Forty-six states use facsimile to transmit election-related materials. Of those states, 23 allow blank ballots to be faxed to voters, and 17 allow voters to return voted ballots by fax. Of those 17 states, 9 restrict the use of fax to military personnel or to emergencies and special cases of overseas voters. See the Federal Voting Assistance Program (FVAP), "Make Your Mark: 2000–01 Voting Assistance Guide" (Washington, D.C.: U.S. Dept. of Defense), [On-line]. URL: http://www.fvap.ncr.gov/ (Accessed Feb. 16, 2001.)

[10]The issue of the "digital divide" first took form in the mid-1990s with the growing introduction of Internet technologies at home and in the office place. In 1995, the Department of Commerce (DOC) conducted a study entitled *Falling Through the Net: A Survey of the "Have Nots" in Rural and Urban America* that first brought attention to the disparity in access to the Internet for high and low income groups. Since then, the DOC and other public and private entities have examined the digital divide. See URL: http://www.ntia.doc.gov/ntiahome/digitaldivide (Accessed April 12, 2001). The existence of a digital divide is not, however, universally accepted as a statistical fact. For example, Roger G. Noll, Dina Older-Aguilar, Gregory L. Rosston, and Richard R. Ross, in *The Digital Divide: Definitions, Measurement, and Policy Issues* (Stanford Institute for Economic Policy Research [SIEPR]) indicate factors other than income (e.g., level of education) that may explain the digital divide. See URL: http://www.ccst.ucr.edu/cpa/bdd/BDDreport/BDD05.html (Accessed Aug. 10, 2001.)

[11]According to press accounts in New Jersey after the election of 2000, voters in wealthy districts used computerized kiosks to cast ballots while those in lower income districts used antiquated systems and technologies. See, for example, Robert Kuttner, "The Lynching of the Black Vote," *The U.S. Prospect* (Dec. 11, 2000), [On-line]. URL: http://www.prospect.org/webfeatures/2000/12/kuttner-r-12-11.html (Accessed March 12, 2001.)

Security. The integrity of the electoral process is paramount in a democratic society. Actual—or even perceived—manipulation of votes can erode public confidence in government. The tally of votes in the presidential election of 2000 led to concern for integrity and security. Protecting the integrity of elections is a major challenge to Internet voting. Examples of Web-based attacks include the distributed denial-of-service attacks in February of 2000[12] and the more recent "Code Red" and "NIMDA" self-propagating worms. Such attacks demonstrate how hackers are able to manipulate, disrupt, and corrupt computerized systems. If hackers or other malicious actors can manipulate the results of an election (or even claim to be able to do so), then voters and candidates may question the results. Securing the Internet to support elections, from the casting of ballots to the tabulation of results, is crucial to establishing public confidence.

Privacy. With the introduction in 1888 of the Australian, or secret, ballot to ensure free and fair elections, an expectation of privacy became essential to U.S. elections.[13] When a vote is held secret, it is difficult for voters to be strong-armed, corrupted, or bribed, and they are free to vote their conscience without disclosure to government, political parties, or any other entity. The Internet's ubiquity and interconnectedness raise some questions: Can the secrecy of digital ballots be protected without compromising a voter's privacy? Can on-line voting be monitored by outside parties?

Technology. The Internet and other advanced information technologies allow new types of transactions, commercial as well as with friends, family, community, and elected officials. As confidence in and an acceptance of Internet technology grow, citizens may request—even demand—to use the Internet to cast ballots. Given the shortcomings of the present electoral system, the need to improve it by updating the underlying technologies has moved into the foreground. One option for improvement is to use the Internet, but that, again, raises questions: Will the Internet prove sufficiently reliable to support on-line elections? Will voters and election officials be sufficiently proficient in the new technologies to accept that the votes were properly submitted and counted?

Civic Participation. The United States was founded as a representative democracy, a form of government based on the power of civic participation, which is the power of individual citizens to participate in their governance by voting. Citizens elect representatives empowered to make

---

[12]In February of 2000, some of the most popular sites on the Internet, among them Yahoo™, e-Bay™, and CNN, experienced a series of distributed denial of service attacks. DDOS attacks often involve programs that send unending requests to specific Web sites causing access and service disruptions. For information on DOS attacks, see "Denial-of-Service Attacks: Understanding Network Vulnerabilities," IBM Corporation, 6-12, [On-line]. URL ftp://www6.software.ibm.com/software/security/dos.pdf (Accessed April 25, 2001.) See also Dorothy E. Denning, *Information Warfare and Security* (New York: Association for Computing Machinery [ACM] Press, 1999), 41-42, 231-239.

[13]"In 1888 the Massachusetts state legislature initiated remedial action, adopting legislation that provided for the so-called Australian ballot in state elections." See Encarta, [On-line]. URL: http://encarta.msn.com/find/Concise.asp?z=1&pg=2&ti=761555363&cid=5 - p5 (Accessed Aug. 1, 2001.)

decisions and law. The Internet offers individuals increasingly direct access to their elected representatives and to new channels of action, such as on-line polling and mass electronic mail (e-mail) messages with which to satisfy political objectives. But is the United States moving toward a more direct, possibly reactive form of democracy? Will the ubiquity of the Internet push the country toward national plebiscites on major issues? Will the capacity to vote over the Internet increase voter turnout?

2.5 Varying Views of Internet Voting

Views vary widely in debates on Internet voting. Generally, since first surfacing as an issue in 1999, three schools of thought have formed (see **Table 2-5**). The first is that of *technology enthusiasts*, who claim that Internet voting is an inevitable evolutionary outcome of the electoral process. Consisting largely of several dot-com startups, such as election.com and VoteHere.net, and their technology partners,[14] technology enthusiasts believe that the growing public acceptance of e-commerce, its ease of use, and rapid innovations in technology will lead voters to embrace the idea of on-line voting.[15] Acknowledging such significant challenges as security and equal access, the enthusiasts envision a transformation of how U.S. voters will vote and how they will participate in the political process. Their enthusiasm is based on the belief that the Internet promises both to change how citizens interact with their elected representatives and to stimulate voter turnout among young, technology-savvy voters.[16]

At the other end of the spectrum are the *critics* of Internet voting, composed largely of public interest groups and Internet security experts. Those critics argue that Internet voting is based on nascent technologies that have significant security vulnerabilities[17]; that these

---

[14]Dot-com vendors of on-line voting technologies have significant strategic and technical partners. VoteHere.net, for example, has partnerships with Compaq, Cisco Systems, and Entrust (a managed security services firm); see URL: http://www.votehere.net/partner.html (Accessed Sept. 3, 2001).

[15]According to John Chambers, president and chief executive officer (CEO) of Cisco Systems, Inc., "The Internet has already changed business in ways no one could imagine just three or four years ago. And we'll look back three or four years from now, and we'll realize that it will have the exact same effects on democracy, politics, and the elections at a pace that many of us may not be able to imagine…" From his remarks on "Internet Voting and Digital Democracy" at "The Future of Internet Voting," a symposium cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, Washington, D.C., [On-line]. URL: http://www.brookings.org/ (Accessed April 12, 2001.)

[16]Ibid. In addition, Steve Case, chairman of the board of U.S. Online–Time Warner, stated: "It's my personal belief that the Internet has the potential to be a democratizing—not a divisive—force. It can enable us to improve the lives of people around the world, with reduced barriers to entering world markets, increased economic prosperity, and enhanced educational opportunities." For the full text of Case's speech to the Congressional Black Caucus, Sept. 14, 2000, see [On-line]. URL http://www.aoltimewarner.com/press/speeches/case/case091400.html (Accessed April 23, 2001.)

[17]For a detailed description of security vulnerabilities associated with Internet voting, see Avi Rubin, "Security Considerations for Remote Electronic Voting over the Internet," AT&T Labs, [On-line]. URL: http://www.avirubin.com/e-voting.security.html

technologies could lead to an increase in fraud, abuse, and vote tampering[18]; that they have the potential to violate voters' privacy and the secrecy of the ballot; and that they might discriminate against voters of less means and with less education.[19] The problems in the national elections of 2000 only reinforced the critics' opinion that the time for Internet voting has not yet arrived.

In the middle ground of the debate are *guarded optimists*, consisting largely of elected representatives, state and local election officials, and social scientists. Guarded optimists recognize that Internet voting is consistent with other efforts to streamline government and are encouraged by its potential for generating constituents' interest and increasing voter turnout. Yet many of them remain concerned about the difficult issues of security, privacy, and the digital divide raised by Internet voting.[20] Such concerns inspired California to create a task force on Internet voting comprised of election officials, vendors, and other stakeholders. The task force recommended an incremental, rather than an abrupt, approach to initiating Internet voting, a view generally favored by many in the state and local community. This approach would allow time to test Internet voting prototypes and technologies, build public confidence in the new procedures, and allow voters to develop trust in them.[21] Events in Florida and other states in the national election of 2000 reinforced the view of guarded optimists that a careful, considered introduction of Internet technologies was the appropriate course of action (for a description of the findings of several election reform initiatives on Internet voting, see **Appendix B**).

2.6 Internet Voting Initiatives

Even before the national elections of 2000 revealed shortcomings in the electoral process, efforts to study and experiment with Internet voting had been undertaken at federal, state, and local levels. This section reviews some key Internet voting initiatives, indicated in **Table 2-6**, which are discussed in later chapters (see also **Appendix B**).

---

[18]Several organizations have voiced concerns about security and fraud in commenting on Internet voting, among them the Center for Public Integrity, a nonprofit that focuses on government accountability, which commented on a project for voting over the Internet conducted by the Federal Voting Assistance Program (FVAP) in a special report that pointed to concerns raised by security experts after dissemination of the "Code Red" worms. The report also addressed the concern that votes could be tampered with, altered, or otherwise invalidated; see URL: http://http://www.public-i.org/story_01_080901.htm (Accessed Sept. 6, 2001.)

[19]For more information on the concerns of critics of Internet voting such as access and security, see Deborah M. Phillips, "Are We Ready for Internet Voting?" [On-line]. URL: http://www.voting-integrity.org/projects/votingtechnology/internetvoting/ivp_0_toc.shtml (Accessed Aug. 23, 2001).

[20]Remarks of Governor Gray Davis of California at "The Future of Internet Voting" illustrate this dichotomy: "I am convinced that within five to seven years Americans will be casting their ballots over the Internet, just as easily as they can buy a stock on e-Trade today. We are not there yet, so we have to find ways to secure some very basic U.S. concepts…personal privacy…and security."

[21]Office of the Secretary of State, California Internet Voting Task Force, "Internet Voting Report," Jan.18, 2000, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/final_report.htm#final-1 (Accessed May 2, 2001.) See also Appendix A of the report, Technical Committee Recommendations, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/appendix_a.htm

Table 2-5

Three Views of the Broad Issues of Internet Voting

	Technology Enthusiasts	Guarded Optimists	Critics
On Internet voting	The Internet is a powerful and democratic instrument that will energize voters.	Internet voting is consistent with efforts to streamline government but must be developed incrementally.	Internet voting will exacerbate the digital divide and is based largely on untested, nascent systems.
On access	Internet voting will improve the average voter's access by offering alternative means for casting ballots.	Although Internet voting may exacerbate the digital divide in the near-term, eventually it may improve access and citizens' acceptance of Internet technologies.	Internet voting favors voters with greater means, that is, access to high-speed computers and Internet service providers (ISPs).
On security and privacy	Security and privacy are important but can be resolved by technical solutions already in use in the commercial realm.	Security and privacy require an incremental approach to test systems and ensure that individual ballots will remain secret and secure.	Security and privacy are absolute requirements for elections. Internet elections should not be conducted unless an election can be made "perfectly secure."
On technology	Growing public acceptance of and confidence in Internet technologies will lead to growing demand for access to Internet voting.	Internet technologies promise to improve the electoral process, but improvements need to be made incrementally.	Internet technologies are not reliable and may be disadvantageous to those without access to or experience with on-line applications.
On civic participation	The Internet provides new ways for citizens to vote, to interact with their representatives, and to discuss issues.	The Internet empowers the individual voter, but it also raises questions about direct vs. representative democracy.	The Internet opens up prospects for plebiscitary or reactive forms of democracy in the United States.

Source: Booz Allen Hamilton.

An event that proved crucial to the debate about Internet voting was the national election of 2000. The problems encountered in the presidential race in Florida and New Mexico, as well as in some Congressional races, are shaping consideration of Internet voting. With increased attention to electoral processes, calls for election reform, and reports from several task forces on election issues at the national and state levels, Internet voting has become a subject of national inquiry. The broad issues raised by the prospect of Internet voting are examined in the following five chapters.

Table 2-6

Significant Internet Voting Initiatives

Initiative	Description
University and school trials 1999–2000	In 1999 and 2000, high school and college students across the United States participated in mock elections, including presidential preference primaries and binding student government elections conducted over the Internet. For example, over two days (March 6-8, 2000) students at Kansas State University participated in a binding election conducted over the Internet to elect officials to the student governing association.
California Internet Voting Task Force January 2000	In 1999, in response to increasing grassroots pressure to consider Internet voting as an alternative to the traditional polling booth, California established a task force of state officials, academics, and leaders from the information technology industry to study Internet voting. The task force issued a report in January of 2000 that recommended an incremental approach to introducing Internet technologies into the electoral process.
Alaska straw poll January 24, 2000	Alaska was the first state to use Internet technologies to support a straw poll vote. Alaskans in three northern districts, as well as the state's congressional delegation, voted over the Internet in a Republican presidential straw poll. In total, 35 of 56 eligible Republican voters took part, voting from home, a public location, or public polling stations.
Arizona Democratic primary March 2000	Arizona's Democratic Party participated in the first binding, statewide Internet-based primary election. Approximately 40,000 registered voters took advantage of the opportunity to cast electronic presidential nomination ballots over the Internet. The primary was significant for many reasons, but one of its most important aspects was a lawsuit brought by the Voting Integrity Project concerning equal access for minority voters.
National party conventions July–-August 2000	In 2000, the Democratic, Republican, and Reform parties all considered limited experiments with on-line voting at their convention sites. At the Democratic national convention (Aug. 16-19), various technologies were used to conduct the first "e-Convention." Delegates were able to cast on-line nomination votes for the nominee, Al Gore. At the Republican national convention (July 31-Aug. 3), an on-line system was provided for use on the convention floor, but, in the end, it was never used. For the Reform Party national convention, remote Internet voting was offered as an option for delegates, but the tumult and division within the party caused by the nomination of Patrick Buchanan complicated efforts to use the system.
NSF symposium and report October 11-12, 2000	The National Science Foundation, in conjunction with the Internet Policy Institute, sponsored a symposium on Internet voting. The symposium brought together computer security experts, social scientists, election officials, archivists, and vendors to consider the implications of Internet voting, identify critical issues, and define an agenda for future research. The NSF issued its Report on the National Workshop on Internet Voting: Issues and Research Agenda on March 6, 2001.
ICANN elections October 2000	The Internet Corporation for Assigned Names and Numbers allowed its at-large members to vote over the Internet to select five new directors of the corporation. More than 75,000 members over the age of 16 attempted to participate and cast on-line ballots.
Federal Voting Assistance Program Election Day November 2000	A small pilot project called Voting Over the Internet (VOI), managed by the Federal Voting Assistance Program, extended Internet registration and voting to 84 voters covered under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986. The VOI project was designed as a registration and ballot-delivery system that replicated mail-in absentee ballot procedures used by local election officials. Participants included out-of-state and overseas military personnel, their families, and other U.S. citizens living abroad who came from participating counties in Florida, South Carolina, Utah, and Texas.
Internet voting trials in California and Arizona Election Day November 2000	California and Arizona conducted independent experiments on Election Day using Internet-based voting in trial elections. In Arizona, one vendor offered on-line voting as a trial at local polling places. The California trials were intended to test different technologies and approaches developed by vendors. Three vendors participated to allow voters to cast nonbinding ballots from on-line voting machines in polling places in four California counties.

Chapter Three

Access

The history of the electoral rights of the poor, nonwhites, and women in the United States is long and filled with controversy. The women's suffrage movement at the turn of the twentieth century and the long civil rights campaign to secure the franchise and ensure equal access to the ballot box were among the largest social movements in U.S. history. The Constitutional and other legal protections that emerged from these struggles offer the clearest view of the role of the federal government in national elections. The Constitutional protections embedded in the Fifteenth Amendment and in such federal laws as the Voting Rights Act of 1965 were intended to prevent voter discrimination based on race or gender. Federal and state governments have issued regulations to ensure assisted voting and poll accessibility to aid illiterate, elderly, and disabled voters. All of these protections are rooted in the belief that every eligible voter must have access to the polls to exercise the right to vote.

Equal access to the ballot box was a major issue in 2000, perhaps most obviously in Florida but also in other states, such as New Jersey and Missouri, where poor and minority communities were required to use old voting equipment and to wait in long lines to vote.[1] By spotlighting voter disenfranchisement owing to faulty procedures and equipment, the national election showed that, even with the current election laws and other legal protections, difficulties remain. Events in Florida showed, and the outcome reinforced, that real and perceived disparities in access can lead to questions about the legitimacy of an election.

This election also emphasized problems that accompany the concept of Internet voting. Internet voting raises questions about fairness and access, specifically, about the digital divide between cyberspace "haves" and "have nots."[2] Although voter turnout and convenience may benefit from Internet voting, would Internet voting disproportionately give the wealthy greater influence over the outcome of an election through voting on-line than less affluent voters, waiting in long lines at poorly equipped and possibly faulty polling stations, would have? Without uniform access to the Internet and supporting technologies, would discrepant access to computers

---

[1]Press accounts in New Jersey that followed the election of 2000 described the way voters in wealthy districts used computerized kiosks to cast ballots while those in lower income districts used antiquated systems and technologies. See, for example, Robert Kuttner, "The Lynching of the Black Vote," *The U.S. Prospect* (Dec. 11, 2000), [On-line]. URL: http://www.prospect.org/webfeatures/2000/12/kuttner-r-12-11.html (Accessed March 12, 2001.) In addition, it was widely reported on Election Night that polling stations in Dade County, Florida, and East St. Louis, Missouri, were kept open past the ordinary hour of closing in order to accommodate long lines of voters waiting to vote.

[2]The issue of the digital divide emerged in the mid-1990s, when Internet technologies began to be used in the home and office, although the statistical evidence for its basis in income, race, level of education, and other factors remains a subject of debate. The concern is that wealthy voters who possess the means with which to acquire computer equipment and high-speed Internet access may gain greater access to the digital ballot box.

and the Internet introduce uncertainty about full and equal participation in elections? If inequities in access and fairness emerge, who should bear the responsibility for alleviating them, the federal government, the states, municipalities and localities, or private industry?

3.1 Could Discrepancies in Access to Computers Affect the Validity of Internet Elections?

Critics of Internet voting such as the Voting Integrity Project (VIP), a national voters' rights organization, argue that the digital divide will make it easier for citizens of certain economic classes and races to vote than for others.[3] If the national election of 2000 is an indicator, these concerns may be justified: minorities and the less wealthy were disenfranchised in some precincts and counties. Owing largely to old and poorly maintained voting machines at local polling places in poorer precincts and the long lines at the polls in urban areas, access to voting of less wealthy voters on the whole was not equal to that of voters in wealthier precincts.

The series of three reports by the National Telecommunications and Information Administration (NTIA) called *Falling Through the Net* provides information that supports concern about a chasm between those who have access to computers and the Internet and those who do not.[4] According to the second report in the series, households with incomes of $75,000 or higher are more than 20 times as likely to have access to the Internet than those at the lowest income levels and more than 9 times as likely to have a computer at home.[5] The studies indicate that the fault line of the digital divide is race. For example, although since 1994 ownership of personal computers (PCs) has risen among minority groups, African Americans and Hispanics continue to lag behind the national average. Caucasian households (40.8 percent) remain more likely to own a PC than African-American (19.3 percent) or Hispanic (19.4 percent) households, and 3 times as many Caucasian households have on-line access (21.1 percent) as African-American (7.7 percent) or Hispanic (8.7percent) households.[6] According to the NTIA reports, similar discrepancies hold also for education and age: those with a college education (63.2 percent) are almost 10 times more likely to own a computer than those without any high school

---

[3]The VIP developed several programs about poll watching, monitoring, and registration to educate voters about their rights and to ensure that elections are conducted with integrity. In 1999, the VIP entered public debate on Internet voting with its study "Are We Ready for Internet Voting?" which examined the new threats to voters' rights and to the integrity of elections posed by on-line voting and which concluded that these threats were still too great to move forward with Internet voting; see URL: http://www.voting-integrity.org/ (Accessed May 11, 2001.)

[4]NTIA, *Falling Through the Net: A Survey of the "Have Nots" in Rural and Urban America* (July 1995); *Falling Through the Net II: New Data on the Digital Divide* (1997); and *Falling Through the Net III: Defining the Digital Divide* (1999), U.S. Dept. of Commerce, [On-line]. URL: http://www.ntia.doc.gov/ntiahome/net2/falling.html (Accessed Sept. 13, 2000.)

[5]*Falling Through the Net II: New Data on the Digital Divide*.

[6]Ibid.

(6.8 percent), and seniors account for the lowest use, followed by the very young. The demographic group determined most likely to own a PC is between the ages of 35 and 44.[7]

The implications of these discrepancies may be far-reaching for Internet-supported elections. A high concentration of affluent communities of voters with the option of Internet access and its convenience may slant an election toward candidates who appeal to this demographic group. Minorities, such as African Americans and Hispanics, may be denied equal access (in particular, equally convenient access) to the tools and technologies needed to cast electronic votes, thereby reducing their proportional influence—precisely the claim of minority groups (economic, racial, age) in Florida in the national election of 2000.

The issue of discrepant access specifically related to Internet voting became evident in the Arizona Democratic primary in March of 2000. Arizona's Democratic Party planned the first binding, statewide partially Internet-based primary election, in which registered voters would cast electronic ballots. The Internet-based portion was managed and executed by a private company, election.com.[8] Before the primary, however, the Voting Integrity Project (VIP) filed a lawsuit on behalf of minority voters challenging the Arizona Democratic Party's plan to allow on-line voting in its presidential primary. Filed in Phoenix in the month of the primary, the lawsuit stated:

> Internet voting violates the Voting Rights Act because it provides voting opportunities to some voters but not to all voters. Specifically, the Arizona Democratic Party plan increases the strength of white voters, who on balance have greater access to the Internet, at the expense of African-American, Hispanic, and Native U.S. voters, who on balance have less access to the Internet.[9]

The suit contended that the "Internet voting system planned for the Arizona Democratic presidential primary [would] have the effect of maximizing affluent white participation relative to non-whites in the primary."[10] The presiding judge was quoted as recognizing that Internet voting may "result in racial discrimination in this election," but let the election take place, stating that the results could be discarded if it were determined that Internet voting significantly skewed voter

---

[7]Ibid.

[8]James Ledbetter, "Arizona Democrats, Online Voting," *The Industry Standard Magazine* (March 10, 2000), [On-line]. URL: http://www.thestandard.com/article/0,1902,12858,00.html (Accessed April 24, 2001.) See also "The Red Herring 100 Company Profiles," *The Red Herring* **79** (June 2000), 144, 356.

[9]Press release, "VIP Will Not Appeal Judge's Decision Allowing Internet Primary to Proceed but Will Fight Onward with Voting Rights Act Claim," Voting Integrity Project, March 3, 2000, [On-line]. URL: http://www.voting-integrity.org/text/2000/rel030300.htm (Accessed March 17, 2000.)

[10]Ibid.

demographics.[11] Although a federal court did not permit the lawsuit to prevent Internet-based voting in the primary, the questions raised in the suit linger.

According to Professor Michael Cornfeld of George Washington University, who studies the role of the Internet in politics, although Internet voting is not illegal, it "runs counter to the principle that electoral access should be equal and universal."[12] Cornfield points to Madison's question in *Federalist* 57, "Who are to be the electors? Not the rich, more than the poor; not the learned, more than the ignorant."[13] In the Arizona primary, according to Cornfeld, this principle was "offended" by Internet voting.[14]

Internet voting advocates, however, such as election.com, believe that providing voters with more choice in how to vote will increase access and voter turnout. According to Joe Mohen, then president and CEO of election.com, computers are cheaper than traditional voting machines, and their lower cost would enable election officials to set up polls in public places, such as shopping malls and public schools,[15] to offer convenient voting venues for those who do not have PCs at home or other easy access to them or to the Internet. This would increase opportunities and convenience even for less affluent voters by increasing the number of polling places and thereby reducing the time spent waiting in line to vote.

There are other instances, such as in rural, geographically dispersed communities, in which on-line systems facilitate greater access. Advocates point to the Alaska straw poll in January of 2000, in which registered Republicans cast votes over the Internet from home or from a public location or public polling station, as an example of how the Internet can help promote access. According to Thomas McKay, chairman of the Alaska Republican Party, quoted at the time of the straw poll, "There has been a high level of interest and excitement over this project. Many people in the bush feel neglected, and we are trying to counter that perception by using this breakthrough technology to bring democracy to their doorsteps. Due to natural barriers, it has been difficult for these U.S. citizens to participate in the democratic process."[16] Alaska offers an extreme example of a highly dispersed electorate, vast distances, and formidable geography, but a useful one of how Internet voting can increase physical access to the voting booth beyond what traditional methods and technologies can offer.

---

[11]Ibid.

[12]Ibid.

[13]Ibid.

[14]Ibid.

[15]Anick Jesdanun, "Arizona Proceeds with E-lection Despite Doubts," *The Augusta Chronicle*, March 5, 2000, [On-line]. URL: http://www.augustachronicle.com/ns-search/stories/030600/tec_124-8547.shtml (Accessed March 6, 2000.)

[16]Press release, VoteHere.net, "VoteHere.net to Conduct First Binding Internet Election", Dec. 10, 1999, [On-line]. URL: http://www.votehere.net/news/archive99/121099.html (Accessed July 3, 2001.)

Further, acceptance of arguments based on a digital divide is far from universal. Critics question the underlying statistical data used in support, regarding the media as emphasizing bad news rather than good. According to David Boaz of IntellectualCapital.com, a weekly public policy e-journal, the extent to which a "racial ravine" exists depends on one's interpretation of the statistics.[17] For example, according to the findings of *Falling Through the Net III* (1999), between 1994 and 1998, for households with computers the gap between Caucasians and African Americans grew by 39.2 percent.[18] Boaz argues that same raw statistical data used to reach this finding might be interpreted to indicate other results. The data could be said to reveal for the same years a gap between Caucasian and African Americans that grew from 16.8 to 23.4. Looked at another way, the same data could be said to indicate that in 1994 Caucasians were 2.6 times as likely to have a computer as African Americans but in 1998 only 2.0 times as likely to have one.[19] Pressing this argument further, Boaz claimed that still another interpretation could indicate that from 1994 to 1998, ownerships of computers by Caucasians grew 72 percent while for African Americans it grew 125 percent![20]

Critics have also pointed to good news about Internet access. Where look at the growing gulf between the "haves" and "have nots," in 1998 *Falling Through the Net III* reported that "the number of Americans connected to the nation's information infrastructure is soaring."[21] This growth covers all ages, races, incomes, and educational demographics and suggests a national trend toward general acceptance and use of as well as access to the Internet and computer technologies.

3.2 Who Should Alleviate Concerns About Equal Access and the Digital Divide?

Some combination of federal, state, local, and private assistance will probably be necessary to alleviate concerns about equal access. Each level of government already plays an important role in the electoral process. The federal government oversees elections to ensure that equal access is not denied to citizens in the basis of race, gender, age, disability, or other factors. In some states, such as Texas and Florida, the U.S. Department of Justice oversees ballot development and other election processes and procedures to ensure that new immigrants are not denied their right to vote by language barriers. State governments have varying roles in the management of elections, but, generally speaking, they establish statewide procedures and standards, certify elections, and, in some states, manage centralized registration rolls. Local

---

[17]See David Boaz, "A Snapshot View of a Complex World," Intellectual Capital.com, July 15, 1999, [On-line]. URL: http://speakout.com/activism/opinions/4067-1.html (Accessed Sept. 5, 2001.)

[18]NTIA, *Falling Through the Net III: Defining the Digital Divide* (1999), 8.

[19]Boaz.

[20]Ibid.

[21]*Falling Through the Net III*, 8.

governments are where the "rubber meets the road" in elections. Local governments manage and staff polling stations, design ballots, and tally precinct results. Private corporations, too, have an important role: they supply the voting equipment for state and local governments. Given the relatively static nature of current electoral processes and systems, the role of each entity is quite well defined. But how will these roles change as the Internet and other computer technologies increasingly pervade the electoral process?

The federal role in ensuring equal access to the polling booth will undoubtedly be affected by the prospect of Internet voting. Historically, the mission of the Justice Department is to oversee state and local governments to ensure that no barriers to voting are erected. With the introduction of the Internet, the calculus changes. For example, although the federal government can maintain equal access and ensure there are no barriers to voting at a physical polling booth, how can it ensure equal access for voters logging on at computers to cast electronic ballots? Will voters with newer, faster computers have an advantage? Will rural regions and highly urbanized, less affluent areas receive the same level of Internet service as the high-profit segments of society serviced by ISPs?

In part to mitigate concerns about equal access to information technologies and services, Congress established the "E-rate program" as part of the Telecommunications Act of 1996. This program requires telecommunications carriers to provide commercially available telecommunications services and Internet access to schools and libraries in economically disadvantaged communities at a discounted rate (up to 90 percent). The program has granted funds to more than 85 percent of the initial applicants. A recent (2000) report found that 63 percent of school classrooms were hooked up to the Internet, more than 20 times those wired in 1994.[22] Although the e-rate initiative does not place a computer in every home, it seems to make some headway in closing the divide at the community level.

The digital divide has received acknowledgement from state houses, Congress,[23] and the White House. As early as December of 1999, President Clinton announced several initiatives. Specifically, he requested the National Science Foundation (NSF) to offer grants for research into issues of digital governance, among them the digital divide and Internet voting.[24] In the spring of 2000, he acknowledged that the digital divide also required national attention:

> Today, we're in another time of fundamental economic transformation but we can do it very differently because, unlike the railroads of the Industrial

---

[22]Kenneth Cooper, "Schools' Next Cyber-Step: E-Literacy," *The Washington Post*, June 9, 2000, A-31.

[23]As of late 2001, the administration of President George W. Bush had not announced any formal position on the digital divide.

[24]Remarks by President William J. Clinton, "Bridging the Digital Divide," The White House, Dec. 9, 1999, [Online]. URL: http://clinton6.nara.gov/1999/12/1999-12-09-remarks-by-the-president-on-bridging-the-digital-divide.html (Accessed June 13, 2001.)

> Age, the trade routes of the information age can run through every city, every town, every community. And, in fact, the more communities they run through, the better it works. No one has to be bypassed this time around. The choice is in our hands. We can use new technology to extend opportunity to more Americans than ever before; we can truly move more people out of poverty more rapidly than ever before, or we can allow access to new technology to heighten economic inequality and sharpen social division.[25]

The states have raced to implement initiatives to wire communities and adopt "technology friendly" policies that offer two tangible benefits. First, adopting technology-friendly policies can increase convenience for citizens and lower the cost to the state of services for citizens. Second, such policies demonstrate to private businesses looking for attractive locations the commitment of the state to high technology. Evidence of state investments in technology programs is pervasive. According to Governor Gray Davis of California, for example, that state has spent $364 million to wire every high school and plans next to wire every middle and elementary school.[26] Several states have begun to take the initiative in centralizing voter registration using electronic databases to increase efficiency and accuracy. Several localities, states, and even regions have started to pool resources to become more attractive customers for acquiring high-technology services and technologies.[27]

States are the likely focal point for alleviating concern about access for Internet voting. According to Anthony Corrado, professor of political science at Colby College, in addition to implementing laws and election rules for Internet voting, states should bear the responsibility for expanding and facilitating access to the supporting technology.[28] Because county election offices are not likely to have the requisite technical expertise, resources, and budget to expand access, a growing burden appropriately rests on the states.

For their part, local governments are at the center of initiatives for conducting Internet voting. Counties, municipalities, and other local governments are central to the administration

---

[25]Remarks by President Clinton, Digital Divide Discussion with the East Palo Alto Community, Palo Alto, Calif., April 17, 2000, [On-line]. URL: http://clinton4.nara.gov/WH/New/New_Markets-0004/20000417-4.html (Accessed June 13, 2001.)

[26]Transcript of "The Future of Internet Voting," a symposium cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, Washington, D.C., [On-line]. URL: http://www.brookings.org/ (Accessed April 12, 2001.)

[27]For example, Delaware, Maryland, New Jersey, and Pennsylvania have established a "smart technology region," known as HUBS—Hospitals, Universities, Businesses, and Schools—which is intended to boost connectivity across these communities, promote business growth, and upgrade education through high-end technologies. See URL: http://www.usmh.usmd.edu/tfhsn/hubs/sld001.htm and http://www.washingtontechnology.com/news/1_1/daily-news/16374-1.html [(URLs accessed Dec. 12, 2001.)

[28]Maureen Cosgrove, "E-Voting: States Better Get Ready, Experts Say," Stateline.org, Jan. 24, 2000, [On-line]. URL: http://www.stateline.org/story.cfm?storyid=59442 (Accessed March 25, 2000.)

and execution of elections. The resultant highly decentralized and heterogeneous system that emerged in the United may, in part, be blamed for the technical failures and problems of access that arose in Florida in 2000. But how will local governments administer and manage elections in order to ensure equal access when Internet technologies are introduced? Faced with limited budgets and small staffs, local governments are posed a considerable challenge. For local election offices, ensuring citizens of a uniform level of access to technology and sufficient training to use the system, and ensuring sufficient training also to poll workers so they are able to respond to citizens' inquiries (and, for Internet voting, perhaps to staff at on-line help desks), all will require new knowledge, new skills and abilities, and new resources.[29]

The role of private corporations in closing the digital divide and improving access is somewhat controversial. There is little doubt that private companies, the innovators and purveyors of the Internet and computer technologies, will be critical to closing the digital divide. For example, in 2000 the Ford Motor Company announced a program in partnership with PeoplePC, Hewlett Packard, and UUNet to provide eligible employees worldwide with a computer, a printer, and Internet access at home for around $5 a month.[30] Such private sector initiatives, even though they do not include the general population, still can help link a broad spectrum of society with the Internet without the necessity for federal, state, or local funding.

The motivation of corporations, however, remains a concern. For many of them, elections and the processes that support them represent a "public good." Offering universal access to an emerging technology generally falls within the realm of public policy. Offering universal access to telephony and electric power service, as those technologies emerged and developed in the twentieth century, was crucial to the economic development of the United States. As voting enters the Internet world, the private sector may have two potential important roles. First, it will be the innovator, developer, and provider of on-line voting services. Several dot-com vendors have emerged (see **Chapter Six**), but a major concern is whether the ability to use on-line technologies will prove to be a new kind of literacy test.[31] Unfamiliarity with Internet technology may unfairly disadvantage certain groups of voters, such as the elderly or less educated. In Florida in 2000, matters that seemed innocuous—such as ballot design—may result in confusion for voters and, ultimately, lead to their disenfranchisement. Whether the Internet may exacerbate such problems through on-line forms and applications remains a concern.

---

[29]For Internet voting, such services may need to include on-line help desks.

[30]Press release, Ford Motor Co., "Ford Unleashes Power of the Internet for Employees Around the World," Feb. 3, 2000, [On-line]. URL: http://media.ford.com/article_display.cfm?article_id=3858 (Accessed March 15, 2000.)

[31]The literacy test is intended to determine whether a person meets the literacy requirements for voting. After the Civil War, in the Southern states literacy tests were used along with other means (such as poll taxes) to restrict the rights freed slaves to the vote. That is, newly freed slaves were denied equal access to the ballot box. See The Columbia Electronic Encyclopedia Copyright © 1994, 2000, Columbia University Press [On-line]. URL: http://www.infoplease.com/ (Accessed Aug. 23, 2001.)

Private sector players often overlooked are the ISPs and the telephone service providers that supply the backbone and "last mile" for Internet access. Although on-line voting applications may themselves raise issues of access, the main issue is availability of high-speed access in traditionally less profitable because less affluent areas, rural and urban. As in the general system that obtained in 2000, in which election systems varied from precinct to precinct, the quality and quantity of service provided by ISPs and telephone carriers also varied. If citizens in lower income areas are offered slower connections than those in higher income areas—connections that create delays or reliability problems—will the Internet really have improved the condition of the electorate, or will it simply mimic and repeat the access problems now persisting in that system?

Chapter Four

Security

Security is one of the most complex issues affecting the prospect of Internet voting. The integrity of an election—both in its conduct and results—is supremely important to a democratic society. Actual or perceived manipulation of votes or results could erode confidence in government. What happened in Florida and New Mexico in the critical hours during and after the national election of 2000 showed how damaging the perceptions of impropriety can be, leading to recounts, protracted legal challenges, and, ultimately, public mistrust of the results.

Using the Internet to cast ballots and tally results raises immediate concern among those who question Internet security. This concern is exacerbated by the exploits of hackers and by malicious acts in cyberspace. For example, in February of 2000 distributed denial of service (DDOS) attacks occurred on several global e-businesses (e-Trade™, e-Bay™), news providers (CNN), and ISPs (Yahoo! ™); and in May of that year, the "I-Love-You" virus was propagated at breakneck speed across the Internet. In July of 2001, security experts warned about "Code Red" worms, designed to attack, disrupt, and take control of the computer systems of major corporations.[1] The use of denial-of-service tools and of rapidly proliferating malicious code and computer viruses has increased doubts about the usefulness of the Internet to carry out important transactions.

If hackers or other computer intruders can—or even can claim to—manipulate election processes, then voters, election officials, and candidates all may question the integrity of an election and the validity of its results. Securing Internet voting processes from the voter's first use of them is crucial, because the voter's initial assessment of the security of on-line voting may influence general confidence in the electoral system. Four important issues that need to be considered when looking at the security of Internet voting are the following: Will Internet voting expose the security of elections to new risks? What level of risk is acceptable? Can the security of e-commerce be compared to the security of Internet voting? Can the integrity of Internet ballots be protected?

---

[1]Worms are malicious computer programs that self-propagate on networks. Typically, they implant code into computers that is subsequently used to support malicious activities by hackers. The "Code Red" worm was designed to initiate a flood of data from infected computers to the White House Web site, essentially denying access to that site. It was also used to deface other Web sites. The "Code Red II" worm (spread later in July) was designed to install "backdoors"—hidden code implanted into a network to allow a perpetrator or other hackers easy access to that network or Web site in the future. Depending on the extent of propagation, a worm can affect Internet reliability and availability in part or in total.

4.1 Will Internet Voting Expose the Electoral Process to New Risks?

A strength of the present voting system often overlooked is the security offered by wide distribution of its processes and infrastructure. If an individual or a group wanted to affect a national election, tremendous resources and coordination would be necessary to manipulate or disrupt the thousands of local precincts that support a national election. Local fraud remains possible, but wholly disrupting a national election seems highly improbable. This raises an important question: could the transition from a "brick-and-mortar" system that characterizes the current electoral process to an Internet-based one change the notion of what is and is not possible in securing elections?

One benefit of today's distributed, labor-intensive system is that it offers thousands of geographically dispersed targets, and these are supported by human redundancies. One area of agreement among both advocates and critics of Internet voting is that the system may prove a more readily identifiable target for external and internal attack than the present electoral process. Conceivably, the Internet may offer more concentrated and visible targets. For example, the transmission of votes over the Internet will introduce new sources of vulnerability into the electoral process such as major telecommunications providers and ISPs, which are the mode of transport from voter to election office. Moving to an Internet-based system may leave the electoral system vulnerable to wide-scale automated vote buying and coercion, activities not likely on a regional or national scale today.

According to the report of the California Internet Voting Task Force issued in January of 2000 and that of the National Workshop on Internet Voting released by the NSF in March of 2001, an Internet-based voting system would be vulnerable to attack by penetration by malicious software and DDOS. The NSF report warned that penetration attacks could target client-server segments of an Internet voting system and use exploited machines to transport malicious code such as Trojan horses and computer viruses. One danger of penetration attacks is that they can occur without detection and can corrupt data before these have been encrypted and transmitted.[2]

Technical countermeasures, such as firewalls and intrusion detection systems, may prove ineffective against sophisticated penetration attacks, which can cloak the intruder's identity and methods.[3] The California Internet Voting Task Force report concluded that, if no preventative measures are taken, "malicious code can easily change the votes on the electronic ballot without the voter's knowledge, reveal the supposedly secret votes to some outside party, or simply prevent a person from voting, possibly leaving him or her with the impression that the vote was

---

[2]NSF, Report of the National Workshop on Internet Voting, March 2001, 13, [On-line]. URL: http://www.internetpolicy.org (Accessed Aug. 23, 2001.)

[3]Ibid.

recorded."[4] These views were supported in testimony offered by Dr. Rebecca Mercuri before the U.S. House of Representatives Committee on Science, Subcommittee on Environment, Technology, and Standards in its consideration of election reform issues:

> Internet voting (whether at polling places or off-site) provides avenues to the entire planet for malicious denial-of-service attacks. If the major software and hardware manufacturers in the United States are incapable of protecting their own companies from repeated Internet attacks, one must understand that voting systems (created by these firms or others) will be no better (and likely far worse) in terms of vulnerability … Off-site Internet voting also creates unresolvable problems with authentication, leading to possible loss of voter privacy, and increased opportunities for vote selling.[5]

In addition to introducing malicious code, network attacks may also permit intruders to modify data in transit, hijack computer sessions, trick victims into revealing important user data (e.g., PINs or passwords), masquerade as legitimate users, or "spoof" the system,[6] thus opening it to fraud, misinformation, and other disruptions that could call the integrity of an election into question. A hacker might penetrate a system and then claim to have changed a thousand votes for one candidate into votes for the other or to have scripted a software program to issue phony votes automatically. Whether or not the hacker succeeded might prove irrelevant if the claim itself were sufficient to require a recount.

The introduction of malicious code into hardware may also allow intruders to monitor the Internet voting system passively, by capturing user data, decrypting weakly encrypted messages, "sniffing" passwords,[7] and analyzing traffic flow. Even were information in transit neither changed nor deleted, the secrecy of digital ballots might be violated. Thus, both active and passive attacks on the network could expose the electoral process to new risks and thereby diminish its integrity.

Denial-of-service (DOS) attacks present a different type of threat. They attempt to disrupt the communications between client and server by flooding the target with more requests than can

---

[4]Office of the Secretary of State, California Internet Voting Task Force, "Internet Voting Report," Jan.18, 2000, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/final_report.htm#final-1 (Accessed Aug. 24, 2001).

[5] Testimony of Dr. Rebecca Mercuri before the U.S. House of Representatives Committee on Science, Subcommittee on Environment, Technology, & Standards, May 22, 2001, [On-line]. URL: http://www.house.gov/science/full/may22/mercuri.htm (Accessed July 26, 2002).

[6]Attempting to gain access to an information system by pretending to be an authorized user. See Randall K. Nichols, Daniel J. Ryan, and Julie J. C. H. Ryan, *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves* (Washington, D.C.: McGraw-Hill, 2000).

[7]Attacking a system by examining the data traffic in order to recover passwords or other sensitive data.

be handled.[8] DOS can prevent voted ballots from reaching their destination, the local election office, and, thus, could prevent a voter from casting a ballot (see section **4.4**).

The availability of malicious software and DOS tools has increased the range of actors who might seek to disrupt an election. Political activists, anarchists, domestic and international terrorists, and even other nations all might pose risks to an Internet voting system. In the present (2002) system, the options of an individual or group seeking to disrupt or manipulate a U.S. election are limited. A group may protest at polling sites or even resort to violence to make a political statement, but the effect would be contained. Moving ballots to the Internet may allow such a group to attempt disruption of an election not just locally but across the country.

Internet voting may also aggravate the danger known as the "insider threat." Disgruntled employees, angry citizens acting as polling officials, and others working at a polling site already pose such a risk. Officials at the polls can allow ineligible voters to vote, can tamper with equipment, or can take other actions that will affect an election. For those desiring to disrupt an Internet-based election, the most viable option might be to bribe officials at key precincts, but, even then, human redundancies and monitoring would limit a bribe's effectiveness. But Internet voting introduces a new "insider threat": the software developer. Internet voting will probably be software driven, and a developer coding key software could be bribed to insert viruses, Trojan Horses, or other forms of malicious code. Because the Internet voting infrastructure will in all likelihood be based on the best commercial products available, a handful of software coders will have intimate knowledge of the proprietary systems that will support it.

4.2 What Level of Risk Is Acceptable?

Critics of Internet voting have argued that the Internet is highly vulnerable and may never be sufficiently secure to support on-line elections. According to the Voting Integrity Project:

> There is little activity on the Net now that suggests how best to approach online voting security. There are a multitude of online voting opportunities on the Internet, but most do not even attempt to offer the level of security that would be necessary for public elections. Even stockholder voting, which is just now taking hold on the Internet, is not a good comparison since its requirements differ from public elections. It is much more challenging to build a system that has to make sure each voter votes only once without revealing who each voter voted for.[9]

---

[8] NSF, Report of the National Workshop on Internet Voting, 14.

[9] For more information, see Deborah M. Phillips and David Jefferson, "Is Internet Voting Safe?" Voting Integrity Project (July 10, 2000), [On-line]. URL: http://www.voting-integrity.org/text/2000/internetsafe.shtml (Accessed April 18, 2000.)

The VIP's criticism of Internet-based voting systems is based largely on assumptions about the Internet's security and its inability to offer protection and security at the level that a mechanical system, such as those now in use, affords.

But is the present system secure? As the difficulties in Florida demonstrated, the average voter has only limited insight into how a vote is captured, transported, tabulated, and stored. Voters usually take the reliability and security of the system as an article of faith—until a problem is revealed. Although Florida suffered national public ridicule for its election problems, for elections it remains one of the most technologically advanced states in the country.

In many respects, the security of the present system is rooted in two fundamental concepts. The first is a model of trust built on redundancy: officials monitor other officials to prevent fraud and abuse.[10] The second is security through obscurity and distribution: the present voting infrastructure is grounded in the most local level of government, with many different processes and procedures, which makes widespread abuse difficult, if not impossible (see **Appendix A**). Although risk is inherent in any type of election, tradeoffs need to be considered to manage it. Acknowledging the weaknesses and risks in the present electoral process, the report of the California Internet Voting Task Force nevertheless adopted the position that Internet voting should not reduce the overall security of elections.[11] To implement Internet voting, manage Internet-related risks, and increase access and convenience for voters, the report recommended a four-stage approach:

- Internet voting at the voter's precinct polling place;
- Internet voting at any polling place in the county;
- remote Internet voting at county-controlled computers or kiosks; and
- remote Internet voting from home, office, or any Internet-connected computer.[12]

Technology enthusiasts may argue that an Internet voting system, properly configured and managed, could offer more secure voting than the present system does, including new protections for voters. The Voting Over the Internet (VOI) project of the Federal Voting Assistance Program (FVAP), for example, used by eighty-four voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA; 1986) for the general election in 2000.[13] In the absentee by-mail process UOCAVA voters use to vote, voters do not appear in person at their local election

---

[10]Based on comments by Jim Adler at "The Future of Internet Voting," a symposium, cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, [On-line]. URL: http://www.brookings.org/ (Accessed April 12, 2001.)

[11]Office of the Secretary of State, California Internet Voting Task Force, "Internet Voting Report."

[12]Ibid.

[13]Federal Voting Assistance Program (FVAP), Voting Over the Internet Pilot Project Assessment Report (May 2001), ES-1, [On-line]. URL: http://www.fvap.ncr.gov/ (Accessed Sept. 5, 2001.)

offices to prove their identities. Instead, they sign a county registration form or Federal Post Card Application (FPCA) and return the form or application to that office by the postal mail system.[14] When the ballot is returned to that office, the local election official compares the signature on file to the one on the ballot to validate the ballot. In this situation election officials need to be able to trust that voters have included valid data on all submitted forms. The nature of UOCAVA absentee voting and the absence of UOCAVA voters, by definition, from their jurisdictions on Election Day led to development of the FVAP as a system that can be used from anywhere in the world. The use of digital certificates permit a voter's identity to be verified, beyond question, and in real-time.[15]

4.3 Are the Security of E-Commerce and of Internet Voting Comparable?

E-commerce transactions and electronic ballots are often compared as analogous types of transactions, but there are three important differences between securing electronic transactions and securing electronic ballots.

First, advocates of Internet voting have been quick to point to the success of e-commerce and the growing public confidence generally in the security of electronic transactions.[16] Critics, on the other hand, have pointed to two distinctions between activities related to e-commerce and those related to Internet-based voting. In commercial electronic transactions, authentication and verification of data are linked. Authentication ensures that those completing the transactions are who they say they are; verification ensures that the content of the transactions cannot be repudiated. In commercial electronic transactions, these acts are inextricable. Internet voting similarly requires that those submitting ballots can be identified as who they say they are and can be authenticated as legitimate users of the system. But once these data have been verified, the identity of the voter must be decoupled from the vote before the voted ballot is opened in order to protect the secrecy of the content.[17] Decoupling adds complexity to the transaction and requires unique technical solutions that can provide for identification and authentication while maintaining the secrecy of the ballot.

Second, as stated in the Technical Appendix of the report of the California Internet Voting Task Force, financial transactions may take place on-line, but a separate off-line process is needed to check the accuracy of on-line activities and to correct errors. In election activities, no such off-

---

[14]Some states do require the FPCA or registration form, or both, to be witnessed or signed by a notary.

[15]Voting Over the Internet Pilot Project Assessment Report, 4-3.

[16]Remarks of John Chambers, CEO of Cisco Systems, Inc., at "The Future of Internet Voting."

[17]According to Jim Adler, of VoteHere.net, "This is not e-commerce, this is not SSL, you cannot solve this with just the methodologies that we have now. To assume that is a huge mistake." "The Future of Internet Voting" symposium, cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, [On-line]. URL: http://www.brookings.org/ (Accessed April 12, 2001.)

line process exists because of the need to maintain the secrecy of the voted ballot. The task force therefore concluded that "the fundamental security emphasis in voting must be up-front prevention of fraud and error, with no reliance on any possibility of after-the-fact correction."[18] Consumer confidence and trust in a voting system are far more urgent than for ordinary commercial electronic transactions: voters will expect high security for the casting of votes for president and other elective offices.

Third, comparisons of electronic transactions and electronic voting differ in terms of value. Although commercial electronic transactions have a finite (monetary) value, voting is a right whose protection under the Constitution and Bill of Rights is priceless.

4.4 Can the Integrity of Internet Ballots be Protected and Secured?

For advocates of on-line voting, adequate technologies and applications already exist to make transactions between voters and the ballot box secure to an acceptable level of risk. Vendors of Internet voting products claim to have developed highly secure systems to protect the integrity and privacy of ballots, and they have begun to apply a variety of them. These range from passwords and PINs to enter Web sites to high-end systems that rely on public key infrastructures (PKI), encryption, and intrusion detection systems. According to John Chambers, CEO of Cisco Systems, Inc., "you can do almost anything with technology now and in the future, so I don't think technology will be our limitation."[19] The most common security solution employed by Internet voting vendors is encryption. Most vendors use secure socket layer (SSL) and other encryption applications in combination with passwords to identify and authenticate users and to secure transactions.[20] In many ways, the system used in the Arizona Democratic primary (see **Appendix B**) resembled the security protections used by Amazon.com and other on-line vendors. A customer (or voter) logs onto a Web site, enters a user identification and password to authenticate identity, and submits a transaction, for example, a credit card number in e-commerce (a vote in Internet voting) in an encrypted format.

Critics claim that such security solutions are insufficient, in three ways. First, user identifications and passwords to identify and authenticate users assure voter identity far less efficiently than more advanced security tools, such as PKI or biometrics. If user identifications and passwords are distributed to voters through the postal mail, as was done for the Democratic primary in Arizona, the Internet voting system could become vulnerable to fraudulent use by those able to intercept the login information en route to a citizen or those who mistakenly receive another citizen's information.

---

[18]Office of the Secretary of State, California Internet Voting Task Force, "Internet Voting Report."

[19]Remarks by John Chambers at "The Future of Internet Voting."

[20]According to the election.com Web site, the company relies on the use of secure socket layer and password protections to provide an acceptable level of security. See URL: http://www.election.com/ (Accessed Oct. 16, 2001.)

Second, SSL is designed to provide security for point-to-point transactions between a user and a trusted party, regardless of content (credit card payment, vote), but it does not defend against all the risks associated with Internet voting. In a national election, the huge volume of ballot data would be transmitted over public networks connecting voters with local election offices. Public networks are, by their nature, vulnerable to technical failure and malicious attack, and the data traversing them are subject to interception, manipulation, even deletion. Protecting the public network, an essential component of the Internet voting "infrastructure," represents a daunting challenge.

Third, the increasing incidence of DOS attacks has exacerbated problems of security. The DOS attacks on leading dot-coms in February of 2000 targeted the underlying infrastructure, rather than individual transactions, in order to congest, degrade, and disrupt the networks supporting the transactions (see section **4.1**). Although security precautions integrated into Internet voting applications may be sufficient to protect the integrity of individual ballots, a large attack made with DOS tools and techniques could degrade the reliability and availability, and therefore the security, of the underlying Internet infrastructure. Attacks launched several days before an election might be difficult to sustain over a long period and the effect on an election might therefore be small, but attacks launched on the day of an election could paralyze the election process, both regionally and nationwide.

Further complicating matters, if electoral history is any indicator, Internet voting infrastructures will be heterogeneous. State and local governments will choose systems to fit their own requirements. Even if federal, state, or local standards for Internet voting were someday to exist, the voting infrastructure in California might not closely resemble that of Alaska or Rhode Island. Thus, how to ensure adequate security across states and localities to facilitate universal trust in such systems becomes an important issue. Advocates and critics alike agree that the federal government will have a role in setting standards, yet they also emphasize that adherence to standards will be voluntary. Disparities in security among the states may emerge as another issue of the digital divide and result in wariness of, rather than confidence in, the new systems.

Chapter Five

Privacy

The introduction of the Australian, or secret, ballot in 1888 transformed voting in the United States, paving the way toward a system that separated and concealed the identity of the voter from the ballot cast. The change was critical, because secrecy protected voters against the growing use of intimidation and coercion perhaps best exemplified by the abuses of Tammany Hall in New York State. Before the Australian ballot was introduced, the paper ballots in use were developed by the political parties in identifiable forms, color-coded and in different sizes, to enable party bosses and the faithful to coerce and intimidate voters as they entered the polling booths. The secret ballot offered voters protection against these abuses.

In the information age, advanced information technologies make protecting private information more difficult than ever before. Massive computer databases aggregate information on individuals, seeking to identify spending habits, consumer behavior, and preferences practiced. In the realm of the Internet, "cookies" and other automated programs are used to track and profile users as they surf through cyberspace. Cookies allow a Web site server to place information about a consumer's visits to the site on the consumer's computer in a text file that only that Web site server can read. Cookie technology assigns the consumer a unique identifier so that the particular consumer can be recognized on subsequent visits to the site. The site can then call up user-specific information, such as the consumer's preferences, interests, or items clicked on during previous visits to the site.[1]

The prospect of introducing Internet technologies to support voting raises fundamental concerns about both individual privacy and the secrecy of the ballot. On-line breaches of privacy protections may allow the identity of the voter to be revealed and a vote to be matched to an identity. Could Internet voting and the digital ballot inadvertently end the secret ballot? Many political scientists and nonprofit groups that focus on privacy and technology and emphasize the importance of the secret ballot, argue that, for Internet voting to succeed, the voter must have "confidence…that this election is just as legal, my vote was just as secret, my vote was counted, as it was if I passed a paper ballot."[2] To avoid compromising the secret ballot, and eroding public

---

[1]Federal Trade Commission, Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security, May 15, 2000, [On-line]. URL: http://www.ftc.gov/acoas/papers/acoasfinal1.htm/ (Accessed May 17, 2000.) Alleged abuse of cookie technologies prompted a class action lawsuit against DoubleClick, an Internet advertising company that cross-referenced anonymous data about on-line shopping habits with real names and addresses. See Tim Hussey, "DoubleClick Dispute Points to Privacy Issue; On-Line Firm Draws Fire by Collecting User Data," *The Chicago Tribune*, March 6, 2000, C-4.

[2]Remarks by Ann McGeehan, director of Elections, State of Texas, and president, National Association of State Election Directors (NASED), at "The Future of Internet Voting" symposium, cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, [On-line]. URL: http://www.brookings.org/ (Accessed April 12, 2001.)

confidence in the election system, a technological system needs to be developed, maintained, and implemented that would provide for secret elections while also allowing the results to be audited. Two issues concerning privacy and Internet voting are, can the secrecy of digital ballots be protected, and will Internet voting affect other forms of voter privacy?

5.1 Can the Secrecy of Digital Ballots Be Protected?

In the United States, voting is considered a sacred and private act, and voters expect that their political preferences will not be disclosed. The importance of privacy may only increase with the advent of Internet voting. Chief among voters' concerns may be that how they vote should not be used against them or developed into a "profile" for some other use. In an Internet voting system, secrecy must be ensured at three stages of the voting: while a vote is cast, while a vote is in transit over the Internet to election officials, and after a vote has been received, stored, and archived by officials.

The California Internet Voting Task Force found that the integrity and security of the ballot in transit could be ensured by means of digital signatures and encryption technologies and that when a ballot was received at the final server, it could be stripped of the identifying information, decrypted, and printed.[3] Such techniques would make certain that local election officials could not tell how a voter voted. To audit votes, electronic ballots might be retained on the server or on electronic disks, without the voters' identifying information. Audit logs within the system could then be used after an election to see who voted, again, without any identifying data that could associate a particular voter with a particular vote.

This theoretical approach was, in many respects, proved by the FVAP's VOI system, which was based on an encryption process designed to mimic the absentee ballot process (see section **4.2**).[4] By mimicking that process, the identity of the voter was decoupled from the content of the ballot.[5] By using a technology that randomizes a voter's identity the system was capable of balancing the concern about the confidentiality of a ballot against the need for an audit in the event of a challenge or recount.[6] The VOI project was only a pilot and therefore was not specifically designed to test issues related to privacy; and the small sample size in supporting counties might have allowed officials to link a voter with a vote.[7]

---

[3]Office of the Secretary of State, California Internet Voting Task Force, "Internet Voting Report," Jan.18, 2000, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/final_report.htm#final-1 (Accessed May 2, 2001.)

[4]FVAP, Voting Over the Internet Pilot Project Assessment Report (May 2001), 1-3.

[5]Ibid., 3-6.

[6]Ibid., 4-7.

[7]For example, because the FVAP pilot only had one volunteer from Dallas, Texas, one of the participating counties, the secrecy of this volunteer's ballot almost certainly could not be protected. Participants in the VOI pilot were volunteers and signed privacy waivers; see [On-line] URL: http://www.fvap.ncr.gov (Accessed Sept. 6, 2001.)

Despite the potential of these advanced technologies to protect digital ballots, privacy remains a concern. Wide use of cookie technology is a significant problem. Even the allegation that an on-line vendor was—intentionally or not—placing cookies on voters' computers when the voters logged on to the Web site to cast ballots could chill voters' consideration of Internet voting as a viable option. Fear that a software glitch could result in an accidental combination of the database of those who voted and those for whom they voted could deliver a devastating blow to privacy in elections.[8]

5.2 Will Internet Voting Affect Other Forms of Voters' Privacy?

Internet companies in general compile a tremendous amount of personal information about users—such as e-commerce consumers and Web surfers—for analysis and profiling.[9] This information may be collected over several years and then identified with particular users. Interactive media have increased the speed and efficiency of collecting, storing, aggregating, and disseminating the information.[10] Expanded to the realm of politics and voting, such information about voters holds the potential for abuse of basic consumer protections and possibly infringement of basic elements of the privacy and secrecy that voters expect. Some political consulting firms, such as Aristotle International, Inc.,[11] already match voting patterns to the personal information consumers provide when signing up for services or making purchases on-line.[12] Although this activity is legal, the prospect of groups and organizations with less than philanthropic motives getting hold of such information introduces the possibility of new forms of coercion, fraud, and manipulation through revelation of how an individual voted.

The potential for violations of privacy exists throughout the entire electoral process. Privacy is important not only to the specific act of voting but also to voter registration. Vendors of on-line voting technology tout the Internet's capability to enable voters to cast ballots in any district anywhere in the state or nation and, eventually, anywhere in the world. They believe Internet voting will eradicate traditional voting districts and lead to establishment of statewide repositories of voter registration information. Aggregated processes of voter registration used for Internet voting may expose personal information about voters to fraud and criminal use. Such information could, for example, be targeted in the same manner as credit card account numbers used in e-commerce. To illustrate this point, consider the options available to an individual or group interested in altering the results of an election. One option might be for that individual or group to

---

[8]Dan Lerner, " Arizona Holds Key for Vote for E-Democracy," *Financial Times* (London), Feb. 28, 2000, 10.

[9]Ibid.

[10]Toby Lester, "The Reinvention of Privacy," *The Atlantic Monthly* (March 2001), 28-29, [On-line]. URL: http://www.theatlantic.com/issues/2001/03/lester-p1.htm (Accessed Sept. 6, 2001.)

[11]Information about the company is available at its Web site at URL: http://www.aristotle.com/management.asp

[12]John Dickerson, "Point, Click, Win!" *Time* (Jan. 31, 2000), 42.

attempt electronic penetration of a state's centralized voter registration system, then steal identities or create false ones that would allow members of the group to cast, in effect, *legitimate* ballots in an election. At the same time, access to that information might also enable intruders to steal a voter's identity and perpetrate other types of fraud.

Chapter Six

Technology

Since the turn of the twentieth century, technological innovation has played a key role in shaping how voters in the United States elect their leaders. Concerned about growing political corruption and vote tampering, in 1892 New York State introduced the pull-lever machine, which automated voting and made the act of "stuffing the ballot box" impossible. Since then, technology has improved the speed and accuracy of counting, reconciling, and, where necessary, recounting votes. In the national election of 2000, counties in Florida that used old technologies were the sites of the protracted recounts, not counties with more advanced voting equipment. A problem frequently overlooked in the immediate aftermath of the 2000 Election was that, across the country, across states, and even across localities and precincts, different technologies, some more, some less advanced, are used to cast and count ballots (see **Table 6-1**).

Table 6-1

U.S. Voting Systems: Types and Penetration

Voting System	Number of Counties	U.S. Population (%)
Optical Scan Lever Machine	1,217	27.2
Lever Machine	480	18.2
Paper Ballots	410	1.4
Punch Cards	578	32.4
Mixed	141	7.9
Electronic	257	8.9
Datavote machines	57	4.0
Total	3,140	

Source: Booz Allen Hamilton.

Realizing the potential of Internet voting will require addressing many technical hurdles. This chapter looks at the following issues. First and most important, the Internet's infrastructure will need to be seen by both election officials and the voting public as adequately reliable, and Internet voting solutions will need to prove scalable. To date, Internet-based voting solutions have been focused on relatively small pilots and trials used over a few days or a week, not in a single day and by a hundred million voters. Ultimately, the technology-centric issues may be over-shadowed by "human" factors, such as whether election officials and citizens can use on-line

solutions effectively. Understanding how to administer and use Internet technologies in voting may be a greater challenge than strengthening the Internet to support voting.

6.1 Is the Internet Reliable Enough to Support Voting?

In addition to the Internet's vulnerability to computer attacks is its susceptibility to network outages and congestion. Owing to its open, public architecture and to the absence of centralized control or administration of operation, the Internet can lack robustness and reliability. The National Research Council (NRC) report *The Internet's Coming of Age* emphasized that little is yet known about the primary causes of the Internet's unreliability, mainly because the Internet is composed of thousands of distinct networks run by different ISPs. Measuring reliability is complicated, given that ISPs typically do not publicly report outages or the frequency or causes of major failures that affect large numbers of customers.[1] Without this information, learning the sources of reliability problems is difficult, and taking action to improve overall Internet reliability is hindered.

The NRC found that, even with some information on the risks and vulnerabilities of the Internet, what will be needed is a thorough understanding of underlying technologies to support reliable networks in order to develop and implement effective solutions.[2] The multitude of Internet technology vendors, the vast array of Internet products they produce, and the constantly changing "state-of-the-art" Internet technologies all have made it extremely difficult to obtain an adequate understanding of the technologies and their capabilities before these are outmoded. Although technologies to improve the Internet's performance and security are constantly upgraded, overall implementation of protective measures has tended to lag, owing to issues of cost and performance. Implementing adequate end-to-end Internet performance solutions will require close partnerships among competitive ISPs to adopt technical standards, and this, according to the NRC's report, remains a "dim prospect."[3]

The prospect of network congestion and outages may affect the ability of states and local governments to employ Internet-based solutions. If present election procedures and practices were used, voters, unless they qualified for a form of absentee ballot, would cast ballots on Election Day. But can the Internet withstand millions of voters casting ballots within the twelve-hour voting period traditionally offered by polling stations? Even very flexible arrangements, such as expanding the voting period for national elections to several days or a week, might, when added to ordinary Internet traffic (including e-commerce and general Web surfing) result in major

---

[1]National Research Council, *The Internet's Coming of Age* (Washington, D.C.: Committee on the Internet in the Evolving Information Infrastructure, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, 2001), 6.

[2]Ibid, 9.

[3]Ibid, 10.

network congestion and, in the worst case, outages. Another possible complication might be that, in the same period, hundreds of thousands, even, potentially, millions of voters might use the Internet to track election results.

The election of five new directors of the Internet Corporation for Assigned Names and Numbers (ICANN) in October of 2000 illustrates the dilemma of reliability. In one week more than 75,000 members over the age of 16 attempted to cast on-line ballots, but several circumstances—including programming glitches and network congestion—led to complaints from on-line voters.[4] Had this unreliability persisted, losing candidates might have had grounds for protest, something clearly unacceptable in a national election.

6.2 Is Internet Scalability an Issue for Voting?

National elections may require huge Internet capacity if voting is to be restricted to a short period of time. According to the NRC report, in general, as the Internet's user base grows, given insufficient technology or capital, the demand for Internet capacity may well outstrip the ability of vendors to provide sufficient capacity.[5] To meet projected demands for more broadband applications and to support the increasing number of devices connected with the Internet, the Internet will continually need to be scaled up:

> Scaling challenges at all levels, from the Internet's core to the applications that run over the Internet, will require continuing, persistent attention by infrastructure operators, equipment vendors, application developers and researchers.[6]

In addition to overall capacity, scaling will be required for particular features of the Internet, such as the domain name system (DNS), the address space, and the routing infrastructure. The DNS, which provides the Web address to the Internet Protocol (IP) address translation service, is already taxed by the growing number of domain names and name translation requests.[7] Every device connected with the Internet needs an IP address, and the increasing number of users and attached devices may exhaust the address pool.[8] Routing devices, which direct traffic on the Internet, are taxed also by the effort to keep pace with the volume of routing options and constant route updates that need to be processed. All these factors are being examined by infrastructure providers and will need to be addressed to assure adequate reliability of the Internet in the future.

---

[4]James Evans, "ICANN Election Starts with Small Snag," Network World Fusion News, Oct 2, 2000 [On-line]. URL: http://www.nwfusion.com/news/2000/1002icann.html (Accessed April 23, 2001).

[5]NRC, *The Internet's Coming of Age*, 55.

[6]Ibid.

[7]Ibid., 58.

[8]Ibid., 65.

And an immediate problem in applying the issue of scale to Internet voting is how to determine through which device, which connection, and to which server a vote will be cast and transmitted.

6.3 Are End-User Devices Reliable Enough to Support Internet Voting?

End-user devices attached to the Internet may introduce vulnerabilities that could affect Internet-based elections. Common malicious acts—attacks by viruses or Trojan horse software on home or office computers used to vote over the Internet—may yield denial-of-service disruptions on an Internet voting server or an electronic alteration of ballots (see **Chapter Four**).[9] Because the Internet is public and access to it is unrestricted, those with malicious intent and determination can access devices connected with it surreptitiously and disrupt processes or alter or destroy information. Voting over the Internet from home computers is especially vulnerable, because, as the California Internet Voting Task Force found, most home users are either unaware of security hazards that may affect voting or simply may not know how to use the available security tools. The result is susceptibility to attack.[10]

6.4 Will Human Factors Eclipse Technology Issues in Internet Voting?

Until the election of 2000, it appeared fair to assume that the average U.S. voter trusted in the integrity of elections. That election shook this trust. The aftermath of public ambivalence about election procedures may increase the tentativeness of acceptance of Internet voting. Even the early developers of Internet voting applications, such as VoteHere.net, agree that a vital first step toward acceptance is achieving trust in the technology and in the process of Internet voting. According to Jim Adler, CEO of VoteHere.net, elections

> are protected by a distributed system of trust. I have election officials watched by party observers watched by poll watchers, everybody is sort of watching everyone else. There's no one individual or authority that can change the outcome of an election. It's important that an Internet voting system have the same kind of trust model, so that it's distributed trust.[11]

To develop trust in an Internet voting system, a trained and certified staff will be needed to manage the system and provide prospective users, themselves not experts, with a good understanding of the system and how it will work. In short, the efficacy of technical solutions will be limited by the ability—of election officials and voters—to implement, configure, manage, and

---

[9]Office of the Secretary of State, California Internet Voting Task Force, A Report on the Feasibility of Internet Voting, "Internet Voting Report," Jan.18, 2000, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/final_report.htm#final-1 (Accessed May 2, 2001.) See, also, Appendix A, Technical Committee Recommendations, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/appendix_a.htm

[10]Ibid.

[11]Remarks at "The Future of Internet Voting," a symposium cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, Washington, D.C., URL: http://www.brookings.org/ (Accessed April 12, 2001.)

use the tools of the system. Even the most advanced technology, combined with security and privacy features, ultimately cannot offer a "silver-bullet" if the system's operators and users at all levels are not adequately trained to cope with software glitches, hardware failures, and potential security risks. Like all major problems associated with information technologies that business and government encounter as they embrace the Internet, failure to address the training and education of users (both administrators and users) may emerge as the Achilles' heel of an Internet-based voting system.

One significant complication is that every state and locality has its own qualifications for the staff that monitor polling stations and Election Day procedures. The technical complexities of an Internet-based voting system will require both staff and volunteers to be more highly trained and specialized than at present. Such a system may even require a cadre of information technology professionals from the states, consisting of vendors, consultants, and volunteers, to operate the system and to earn the trust of the electorate. The absence of adequate funding and skilled volunteers may prove an immediate and daunting obstacle to Internet voting.

Another impediment to public acceptance of Internet voting may be the public's own lack of awareness of the potential vulnerabilities of the security of Internet voting and of the authentication technologies that might remedy them. An Internet-based system will require, at a minimum, people to provide PINs and user identifications to satisfy concerns about security. It may also require implementation of more complex technologies such as public key infrastructure and biometrics (see section **4.4**). Although these mechanisms may ultimately increase public confidence in Internet voting, they may also increase the challenges for state election offices already operating on tight budgets. Exacerbating matters, insufficient understanding of how hackers, criminals, and others operate in cyberspace may leave voters unwittingly vulnerable to malign attempts at social engineering.

Despite these challenges, Internet voting offers federal, state, and local government an excellent opportunity to educate the public about the benefits of computer technology and to familiarize it with the Internet. Internet voting could, in some ways, provide a springboard for states to use to close the digital divide. By creating on-line alternatives to traditional voting, use of the Internet may encourage citizens to accept and increase their understanding of a technology that has already begun to affect them daily, directly and indirectly. Most important, if correctly implemented, Internet voting could help voters develop a trust in the Internet that may encourage them to take advantage of other government-sponsored Internet-based services and opportunities. Adoption of Internet voting could therefore serve the public good by helping to assuage fears about this communications infrastructure and by accustoming people generally to its use.

6.5 Will Political and Business Considerations Eclipse Technology Issues?

Technology offers potential solutions to the problems of the present electoral system, but three factors complicate efforts to promote Internet voting solutions. The first factor is political

considerations. As the founding fathers intended and the Constitution sets forth—and as Supreme Court's decision in *Bush v. Gore* decision[12] affirmed—elections in the United States remain highly decentralized and distributed. All levels of government have important roles in administering and overseeing elections (see section **3.2**). The founding fathers viewed state oversight of elections as crucial to preventing the emergence of a highly centralized federal government.[13] After the 2000 Election, Congress began to consider a variety of options to reform the nation's electoral systems, some of which envision a stronger role for the federal government.[14] A stronger federal role would be of considerable concern to state governments, which are moving to centralize election-related activities in their own right. For example, states are creating statewide registration databases—and such state efforts might be viewed as usurping local government roles and responsibilities.

Funding is the fulcrum of the debate on the appropriate role of each level of government. Estimates to reform the current electoral system range into the billions of dollars, an enormous burden for cash-strapped state and local governments with other priorities such as schools and transportation. These estimates include only upgrading existing systems with well-established technologies—such as optical scanners and direct recording equipment—and do not factor in the potential costs of on-line voting solutions. For those interested in Internet voting, reaching accommodation on the roles of the different levels of government presents a major challenge.

A closely related point is the political risk associated with implementing Internet voting solutions. For example, one or many states may rush to implement Internet voting for political reasons. A state that wants to demonstrate its willingness to embrace technology might use Internet voting as a "technology showcase" without fully considering the implications. A failed experiment in Internet voting could be devastating, increasing the doubts of those already skeptical about its viability.

This type of situation however, is far less likely to occur than the kind of problem encountered by the Federal Voting Assistance Program in the aftermath of its VOI pilot project. In 1998, the FVAP determined to prototype an Internet registration and voting system and make it available to a selected sample of overseas voters. This involved considerable political risk in two respects. First, VOI was a technical "proof-of-concept" that required a significant investment of time and resources but offered no guarantee of being technically feasible or practical—that is, it could be described as a high visibility, risk-laden research and development (R&D) program. Second, the FVAP took great pains and used many precautions to ensure that no voter would be disenfranchised and it invested in high-end security solutions to alleviate concern about election integrity. Consequently, the VOI system was expensive, costing more than $6 million to develop

---

[12]Bush v. Gore, 531U.S.98 (2000).

[13]For the views of the founding fathers, see Table 7-1.

[14]For a discussion of election reform and Congressional initiatives, see Appendix B.

and field.[15] Even with such efforts, following the successful pilot, the FVAP faced public criticism in some circles for overspending.[16]

The second factor is the business side of Internet voting. Although critics routinely focus on the profit motives of the dot-com vendors, this view fails to take into account the positive impact of innovation and competition. Since the late 1960s, a few entrenched vendors and aging technologies have dominated the election systems marketplace. The entrance of dot-com vendors has already increased competition and forced vendors of traditional election systems to consider new solutions for their customers. Innovative companies, such as VoteHere.net and election.com, secured venture capital and formed strategic relationships with large companies, such as Microsoft and Compaq, among others, to develop, market, and test their systems. But an important question is the long-term viability of the Internet voting marketplace. Specifically, will the dot-coms be able to develop the steady sources of revenue that will allow them to attract further venture capital and strategic partnerships necessary to improve core technologies in what is considered a niche market.

Another factor is the difficulty involved in trying to coordinate large-scale solutions to problems that affect the present electoral system. The development and implementation of Internet voting solutions will require unprecedented coordination across public and private sectors—state governments, counties, municipalities, ISPs, software and hardware vendors, and that end-user, the voter. Traditional boundaries defining public and private roles in elections have begun to blur, and, as election reform and Internet voting initiatives take shape, how the public and private sector partner will be crucial.

---

[15]The VOI pilot project was widely reported to have cost $6.2 million to complete; see: [On-line] URL: http://srd.yahoo.com/goo/%22Internet+Balloting%22/1/*http://www.washingtonpost.com/wp-dyn/articles/A64004-2001Aug11.html (Accessed Sept. 6, 2001.) See, also, URL: http://www.public-i.org/story_01_080901.htm

[16]In a special report, the Center for Public Integrity criticized the VOI project for spending approximately $74,000 per voter to test, field, administer, and evaluate the system; see URL: http://www.public-i.org/story_01_080901.htm (Accessed Sept. 6, 2001.)

Chapter Seven

Civic Participation

At the turn to the twentieth century, the general public increasingly regarded the United States's political system as an "unholy alliance between corrupt business and corrupt politics."[1] In response, massive efforts at social and political reform were mounted, such as the temperance movement, the campaign for universal suffrage, the environmental conservation movement, and the effort to "bust" corporate monopolies. The resulting political and social changes were reflected in changes in the national electoral process:

- Universal suffrage to include women
- Direct election of U.S. senators
- The introduction of initiatives and referendums at the state level
- The use of the secret ballot to eliminate fraud and abuse in voting.

At the turn to the twenty-first century, the dynamic force of the Internet is exerting tremendous pressure on political customs and practices in the United States. The Internet is making more information on candidates and issues available to the average citizen than ever before. Candidates, political parties, grassroots movements, public interest groups, and other political organizations use the Internet to promulgate positions, and citizens use its resources to gather information on candidates and to engage in on-line political discourse. Such use of the Internet—by political parties to raise money, by candidates to mobilize volunteers, and by the public to interact with their elected representatives—raises several questions: Will access to increased information about candidates result in voters being better informed? Is a national plebiscite in the United States's future? Will voting over the Internet increase voter turnout?

7.1 Will Access to Increased Information Result in Voters Being Better Informed?

Carrying the Progressive Era's ideal of the informed citizen into the twenty-first century, the Internet has demonstrated a capacity to inform voters as never before possible. Because the costs associated with registering and maintaining Web sites are very low, compared with those of other means of outreach, groups can use the Internet to provide detailed information on their views of the positions of political candidates at little expense. Potential voters can compare candidates,

---

[1]Progressive Party Platform, Aug. 5, 1912; see Henry Steele Commager, ed., *Documents of U.S. History*, 8th ed. (New York: Appleton-Century-Crofts, Meredith Pub. Co., 1963), 73-75.

review voting records, and engage in informal, grassroots political discussion of a kind not possible with traditional media (radio and television).[2]

Government, the media, and advocacy and political interest groups have placed, and continue to place, enormous volumes of information on the Internet to influence and inform citizens. Although the Internet has the capacity to educate, and thus empower, voters, how best to filter this enormous volume of information has become a concern. As Carolyn Jefferson–Jenkins, president of The League of Women Voters, put it, "Getting information and being bombarded with information is fine, but how do you sort through that, and who do you discuss it with so you can make an informed decision?"[3] Critics have wondered how much of the information gathered can be considered "good." According to Neil Postman*:*

> To say we live in an unprecedented age of information is merely to say that we have available more statements about the world than we have ever had. This means, among other things, that we have available more erroneous statements than we have ever had.[4]

By some estimates, 10 percent of U.S. voters have already used the Internet to gather information that affects their decision when casting ballots.[5] Inevitably, some of it will be questionable in nature and accuracy, but the responsibility of determining the value and usefulness of such information is, as it has always been, the voter's.

7.2 Is a National Plebiscite in the United States's Future?

As recorded in *The Federalist Papers*, Alexander Hamilton, James Madison, and John Jay discussed the design and conduct of elections in the United States with great care and deliberation[6] (see **Table 7-1**). In creating a representative democracy, they established a system that balances energy and stability, a system in which the will (or energy) of the electorate is balanced by the restraint (or stability) of elected representatives. Fundamental to the thinking of the founding fathers as they grappled with developing the U.S. Constitution and a federal structure of governance was the distribution of power. It assumed many forms: between the

---

[2]Center for Democracy and Technology, "Square Pegs and Round Holes: Applying the Campaign Finance Law to the Internet—Risks to Free Expression and Democratic Values," October 1999, [On-line]. URL: http://www.cdt.org/speech/political/financereport.shtml (Accessed Aug. 1, 2001.)

[3]"The Future of Internet Voting," a symposium cosponsored by The Brookings Institution and Cisco Systems, Inc., Jan. 20, 2000, Washington, D.C., URL: http://www.brookings.org/ (Accessed April 12, 2001.)

[4]Neil Postman, *Building a Bridge to the 18th Century: How the Past Can Improve Our Future* (New York: Alfred A. Knopf, 1999), 92.

[5]Center for Democracy and Technology, "Square Pegs and Round Holes."

[6]Alexander Hamilton, James Madison, John Jay, *The Federalist Papers*, edited by Clinton Rossiter (New York: New U.S. Library, 1961). All quotations here from *The Federalist* are from this source.

federal government and state legislatures; between big and small states; and between the desires of the majority and the needs of the few. Out of their considerations grew the complex system of checks and balances laid out in the Constitution. As Madison noted (*Federalist 10*), "the federal Constitution forms a happy combination…the great and aggregate interests being referred to the national, the local, and particular to the state legislatures." This system was tested—and reinforced—by events in the 2000 Election and by the Supreme Court ruling in *Gore v. Bush*.

Table 7-1

The Founding Father's Views of Elections

Issue	Consideration	In Their Words
Representative Democracy	To balance the interests of the populace, a three-pronged approach was created to elect national representatives. Crucial to forming this approach was balancing the opinions of the majority and the needs of the few. The founding fathers feared a tyranny of the majority in a reactionary government or the emergence of powerful classes or political factions. To protect against these possibilities, they advocated the establishment of a system where representatives were elected by popular vote, senators selected by state legislatures, and the president elected by an Electoral College.	Alexander Hamilton: "The House of Representatives being elected immediately by the people, the Senate by State legislatures, and the President by electors chose for that purpose by the people, there would be little probability of a common interest to cement these different branches in a predilection for any particular class of electors." (*Federalist 60*)
Administration of Elections	Against the emergence of a strong central government or, at worst, the tyranny of a king, the founding fathers believed decentralized control of elections afforded the most protection. Consequently, Article One of the Constitution stated that "The times, places, and manner of holding elections for senators and representatives shall be prescribed in each state by the legislature." The founding fathers did recognize a federal role in elections, however, in particular to ensure the unity of the United States.	Alexander Hamilton: "[N]othing can be more evident than that an exclusive power of regulating elections for the national government, in the hands of the state legislatures, would leave the existence of the Union entirely at their mercy." (*Federalist 39*)
Frequency of Elections	To balance the forces of energy and stability in society, James Madison emphasized that the republican form of democracy was preferable, because it contained factions; he argued that the frequency of elections might also either stimulate or regulate the emergence of factions. Annual elections might invite factions and impulsive actions; lengthy terms introduced bureaucracy. Viewing both energy and stability as integral to the new republic, Madison regarded energy as the force of change that would allow the republic to grow; its other face was the potential for a tyranny by the majority. Stability was the force that would protect the republic from other forces, internal and external, seeking to pull it apart, but stability might also allow for the concentration of power. For Madison, the frequency of elections was the means by which to achieve the appropriate balance of energy and stability.	James Madison: "[A]mong the difficulties encountered by the [Constitutional] convention, a very important one must have lain in combining the requisite stability and energy in government." (*Federalist 37*)

Source: Alexander Hamilton, James Madison, John Jay, *The Federalist Papers*, edited by Clinton Rossiter (New York: New U.S. Library, 1961).

Through the initiatives and referendum movements of the 1890s and the public opinion polls of the 1920s, the public acquired an increased role in determining issues and in how politicians responded. Whether directly, through e-mail and "chat" sessions, or indirectly, through on-line polling, the Internet offers the citizen with an opportunity to interact with elected representatives and other government personnel to an unprecedented degree. Electronic messages give candidates and legislators immediate feedback from citizens, who can use this means present their own views, instead of only having elected officials, party organizations, or interest groups do so. Enhanced by Internet technology, opinion polling has become on-line opinion polling, with instant results that have the potential for immediate influence on how politicians respond to events and how they choose to shape their positions and political agendas.

As citizens come increasingly to initiate contact with elected representatives and to rely on the Internet for information, the possibility looms of a direct democracy, or national plebiscite, which could threaten to disrupt that carefully wrought balance. Although the use of the Internet in instant national plebiscites may appear to be the next step in the electronic revolution, the failure of national initiatives and referendum movements in the 1970s suggests that such movements now would face similar uphill struggles.[7]

Regardless, the Internet will probably continue to host many sites that conduct instant polling and offer unscientific results to support their own views. The potential for on-line plebiscites and other political uses of the Internet may force legislators to increase their responsiveness as citizens demonstrate support for a policy or argue against it. Fearful of factions and uninformed choice, the founders of the nation cautioned against fostering such energy, which may today have found a powerful manifestation in the Internet. Were politicians to respond to what may be inaccurate opinion polls and base their actions on the pressure from the masses, the outcome might be precisely what the founding fathers sought to avoid.

---

[7]In December of 1977, the Subcommittee on the Constitution of the Senate Committee on the Judiciary held hearings on two national initiative proposals. The first, introduced by Senators James Abourezk (Dem.-S.D.) and Mark Hartfield (Dem.-Ore.), aimed to provide the people with power to propose and enact laws, except certain powers granted to Congress (declaration of war, calling of state militia). A proposed law would have been enacted on approval by a majority of those casting votes and would take effect 30 days hence. However, a law enacted by initiative could be held unconstitutional by the U.S. Supreme Court and could be repealed by Congress by a two-thirds vote in each house. Another bill, sponsored in the same session of Congress by Representative Guy Vander Jagt (Rep.-Mich.), differed slightly in that a successful initiative would require a majority of votes cast in 38 states, rather than a simple majority of all voters. In addition, a three-quarter vote of both houses of Congress, rather than a two-thirds vote, would be necessary for Congress to reverse the action of the people. Both proposals failed to gather the necessary interest for advancement. See: Richard W. Merriman, Jr., "To Collect the Wisest Sentiments: Representative Government and Direct Democracy," The Jefferson Foundation, 1986, [On-line]. URL: http://www.vote.org/direct.htm (Accessed June 28, 2001.)

7.3 Will Internet Voting Affect Voter Turnout?

As potential voters turn to the Internet to explore the wealth of political information available there, gain opportunities for participation, and find a voice in politics, the question arises of whether the ubiquity of the Internet and, ultimately, Internet voting will increase voter turnout. Proponents of Internet voting contend that easier access to information and to local and congressional representatives ultimately will increase civic participation. According to Jim Adler, CEO of VoteHere.net, "when you bring the source of information closer to the decision, new and different things can happen."[8] Proponents such as Adler appear to believe that the Internet can motivate people to educate themselves and thereby raise interest and foster a desire to engage in the political process. Critics counter that the information available electronically will not increase voter participation. According to Michael Margolis, of the University of Cincinnati, "Where we had hoped to see change possible in the Internet, the net creating a new kind of politics, what in fact we have is politics as usual."[9]

Some critics argue that new campaign technologies and practices may actually contribute to a decline in political participation. The influence of technology-based campaigning has increased, but at the expense of the entrenched political parties. On-line voting applications, such as voter databases, on-line polling, and targeted advertising, which have facilitated communication with voters, have also created a fragmented electorate, thus, these critics contend, lowering voter turnout.[10] The critics view the Internet as yet another technology capable of reducing social interaction and undercutting traditional democratic organizations—the parties, unions, political clubs, and civic groups that once encouraged and taught citizens and promoted participation in political activity.[11]

---

[8]Remarks at the "The Future of Internet Voting,."

[9]Quoted in David Pace, "Internet Not Expected to Expand Voter Participation," Associated Press, [On-line]. URL: http://www.onlineathens.com/stories/052200/tec_0522000013.shtml (Accessed May 28, 2000.)

[10]Marshall Ganz, "Voters in the Crosshairs: How Technology and the Market are Destroying Politics," *The U.S. Prospect* **5**, 16 (Dec. 1, 1994), [On-line]. URL: http://www.prospect.org/print/V5/16/ganz-m.html (Accessed Sept. 11, 2000.)

[11]Ibid.

In the debate on the possibility of casting votes over the Internet, critics are wary of losing the social experience that they believe is a vital component of voting in the United States. In de Tocqueville's view, voting was a public ritual that increased social solidarity and bound people together.[12] Just as television turned generations away from civic participation, so, some political scientists fear, Internet voting may transform an inherently public ritual into a private one.[13] Ordinarily, on Election Day most voters leave home and office, travel to polling places, and physically interact with one another, all on this day being truly equals. Proponents of Internet voting frame their arguments with convenience: enabling busy voters to vote in the comfort of home, or anywhere, for that matter, may revive citizens' engagement with politics. A Harris Interactive poll taken in March of 2000 offered evidence of people's willingness to use the Internet to obtain information about candidates. According to the poll, there were about eighteen million visitors to candidates' Web sites during the primary season, and the top reasons cited for the visits were to learn about a candidate's views on issues, read a candidate's biography, and look at a candidate's schedule of events.[14]

But unless all potential voters have equal access to the Internet and come to accept and trust the technology, Internet voting may not increase voter participation. The debate about voter turnout rests largely on access to the Internet and on issues of security, privacy, and technology.

---

[12]Alexis de Tocqueville, *Democracy in America* (New York: Harper Perennial, 1969), 513-517.

[13]See Robert Putnam, "Bowling Alone: America's Declining Social Capital," *Journal of Democracy* **6**, 1 (January 1995), [On-line]. URL: http://muse.jhu.edu/demo/journal_of_democracy/v006/putnam.html (Accessed July 3, 2001.) In this much debated article, Putnam addressed the decline in civic engagement, linking the erosion of civic participation to technological advances, in particular, the arrival of television and asserting that the act of watching TV in the private sphere encroaches on engaging with others in the public sphere.

[14]Humphrey Taylor, "18 Million Voters Visited Candidates' Web Sites During Primary Campaigns," Harris Interactive, [On-line]. URL: http://www. harrisinteractive.com/harris_poll/index.asp?PID=79 (Accessed April 25, 2001.)

Chapter Eight

Toward a Digital Democracy

The confusion surrounding the national election of 2000 revealed a disquieting paradox: the world's most technologically advanced democracy relies on antiquated machinery. In many states and localities, voters cast ballots by using punch cards, a technology dating back to the 1960s, and in some precincts still by using pull-level machines, introduced in the late nineteenth century. In the aftermath of Election 2000, Congress, state legislatures, and county and municipal governments all have launched efforts to examine how to reform electoral processes and modernize election systems. The Internet increasingly pervades many aspects of life and is championed as an instrument that can empower government, businesses, and individuals.

The allure of the Internet and of its potential to transform how U.S. voters elect their leaders is easy to understand. The Internet would replace obsolete machinery with an information super-highway of networked servers, computers, and "virtual" polling stations. It could enable further automation, which might increase the accuracy of vote tallies. It could streamline electoral processes and procedures, thus improving the efficiency of registration and voting. Yet doubts linger. It might also afford certain segments of society—the disabled and absentee voters for instance—greater access to the ballot box.

This report has attempted to present an even-handed assessment of the debate on Internet voting by identifying and discussing the major issues facing policymakers. Each of them—access, security, privacy, technology, and civic participation—is important in its own right, but four practical conclusions are key to forging a path toward a digital democracy.

First, policymakers, legislators, technologists, social scientists, and others will need to consider Internet voting holistically. Along with such key technical issues as Internet security, reliability, and scale are the equally complex and vexing issues associated with U.S. voting practices and customs, election law, and federalism. Other concerns are economic and budgetary considerations, issues of access and fairness, and questions of how the Internet may transform politics in general. But all these factors may be eclipsed by yet another consideration: voting is a human act, one conducted by human beings, reflecting their principles, strengths, and frailties. For more than two hundred years, from the deliberations of the founding fathers, the changes introduced in the Progressive Era, through the voting reforms of the 1960s, to the adoption of new election technologies, electoral change has always been the subject of intense debate. The reason for this is simple—voting is the ultimate expression of individual liberty and therefore of immeasurable value to every citizen. To compare it to e-commerce is to understate its importance and social relevance.

Second, the distinction needs to be drawn between Internet voting and election reform. In many respects, Internet voting has been miscast as part of larger reform efforts that issued from the national election of 2000. Whereas past efforts at electoral reform were inspired largely by mass social movements or concern about political corruption, and even some present efforts are driven by procedural failures, Internet voting represents a possible transformation of the electoral system that was inspired mostly by technology and is supported mostly by people familiar with technology. Wired citizens, empowered by the multidimensional, feature-rich, information-laden Internet, have pushed for consideration of Internet voting as an alternative to the traditional polling booth. With the Internet now pervasive and almost universally accepted, the technology would seem to sell itself in support of voting from home, work, or school. Enthusiasts envision a new generation of voters energized and mobilized by the ability to vote over the Internet who will reverse the trend toward low voter turnout and voter apathy. But combining these factors with the problems that surfaced in Florida and elsewhere confuses the debate. The push for Internet voting began more than a year before the national election, and it raises policy and technology issues related to but not identical with those of election reform.

Third, each of the issues—access, security, privacy, technology, and civic participation—needs to be studied in light of the electoral tensions that the framers of the Constitution as well as later thinkers have tried to balance, tensions that still exist today. James Madison, for example, discussed the importance of the tenuous balance between energy and stability in society (*Federalist*, 37). Fearful of political factions in society and of citizens making uninformed choices, the framers created a representative democracy to balance the energy and spirit of the masses against the stability of institutions that rely on the consent of the governed. The Internet, which may be seen as the epitome of energy in the information age, is forcefully changing the world. It is easy to get caught up in the enthusiasm for technology and its potential, but the intricate balance of societal tensions that the framers sought to create also needs to be considered as society contemplates the pros and cons of Internet voting.

Fourth, the problems encountered during the national election of 2000 coupled with increased interest in and experimentation with Internet voting may yield two constructive results. The first is the revelation of flaws in the established electoral system, which may reduce resistance to change. In 1999, when work on this report started, one assumption shared by the authors was that voters in the United States accepted, as an article of faith, the integrity of the electoral process. In addition, the authors also assumed that several significant barriers—lack of resources, lack of skilled information technology professionals, and an "if it ain't broke, don't fix it" mentality—would be cited by election officials as obstacles to change. But in the aftermath of the election in 2000, public perception of electoral integrity has, to say the least, become somewhat less resolute. The imperfections exposed have required the public, the media, politicians, academia, as well as state and local election officials to consider carefully what they want to do to reform the election system. Whether their considerations will include the Internet remains to be seen. Internet voting is no panacea, but the problems that occurred in Florida and

other states have introduced a new attention and focus that may well promote careful use of Internet technologies. The practical problems encountered in that election offer a realistic picture of the operating environment in which Internet voting would be introduced. Thoughtful and judicious experimentation with the Internet in key segments of the registration and voting process may incrementally improve the technology and, more importantly, may foster a sense of trust and acceptance among the electorate. Such trust and acceptance are key not only to Internet voting, but to forging a digital democracy.

Appendix A

The Electoral Process in the United States

This appendix on the U.S. electoral process is intended to help readers understand both the particulars and the overall complexity of election activities in states and localities. The intricacy and diversity involved illustrate the difficulty of translating these processes to the Internet. Various stakeholders in the electoral process, from local election officials to state election boards, influence and establish the rules and regulations governing elections, and, further complicating the establishment of new procedures, all of them will have a voice in shaping activities related to Internet-voting initiatives. Long-established processes and procedures will probably provide the foundation for Internet voting efforts and affect the adoption of supporting technologies and policies.

In the United States, the rules that govern election procedures were established the individual states and are maintained by them. The Supreme Court holds that the Constitution preserves the power of the states also for independent election requirements.[1] The role of the federal government is limited to stipulating requirements for certain state election procedures, including ensuring assistance to illiterate voters, access to polling places for the disabled, and the development of bilingual ballots. The Voting Rights Act of 1965,[2] which, with the Fifteenth Amendment, prohibits racial discrimination in voting,[3] provides that states must allow federal observers to attend polling precincts "for the purpose of observing whether persons who are entitled to vote are being permitted to vote."[4] Under federal law, votes for congressional representatives must be cast "by written or printed ballot, or voting machine the use of which has been duly authorized by State law."[5] This provision gives the states the power to establish standards for, and approve the use of, all types of voting equipment.

Various aspects of election and voting processes in the United States are described here, but, because each state has adopted specific, perhaps unique, voting requirements, the examples given here cannot be assumed to apply nationwide.

---

[1]Pamela A. Stone, "Electronic Ballot Boxes: Legal Obstacles to Voting over The Internet," 29 McGeorge Law Review 953, Summer 1998 (referencing Reynolds vs. Sims, U.S. 533, 554 [1964]).

[2]42 U.S.C. § 1971 (1965).

[3]Voting Rights Act Clarification, United States Department of Justice, [On-line]. URL: http://www.usdoj.gov/crt/voting/clarify3.htm

[4]6 U.S.C.A. §1973f (West 1994).

[5]2 U.S.C.A. § 9 (West 1997).

A.1 Voter Registration

The National Voter Registration Act (NVRA) of 1993 established new opportunities for voter registration, but it did not create a national voter registration system—all registration activities are still coordinated locally. The act set out guidelines for registering at state and local government offices and at county and municipal offices and public libraries. Prospective voters can also register when applying for a state driver's license, and most states now post registration forms on their Web sites which can be downloaded.

Those eligible to vote (as determined by state requirements) begin registration by filling out an application form certified by the state and then forwarding it to the appropriate body such as the local election office (LEO) or the County Board of Registration, where the application is processed. The registration office evaluates the completeness and validity of the information on the form and determines whether the requestor is eligible to vote. If the request is approved, the office then forwards a registration card to the new voter indicating the address or location of the polling place for the precinct in which the voter is registered. When a request is denied, a notice is sent to the requestor indicating the reason(s) for denial. If the form is incomplete, a notice is sent to the voter requesting additional information.

The degree of automation of local election offices varies across each state and the country as a whole. Some jurisdictions maintain registration records manually, while others use automated systems that rely on desktop and mainframe computers.[6] Some states use, or are implementing, centralized, statewide systems, typically mainframe computers stationed at local voter registration offices. These computers are connected through a leased commercial network to a mainframe computer that contains the registration database managed by the State Board of Elections (SBE) or some other authorized state entity.

A.2 Voting Equipment

Support services and technologies, as well as actual voting procedures, are locally coordinated. Voting precincts (which are established by counties) are supplied with voting equipment, usually purchased by either municipal authorities or the board of county commissioners. Each state sets the guidelines for levying taxes to raise money for equipment, and the monies collected are placed in a fund. The type of voting machine required by the supervisor of elections for each precinct will depend on the volume of registered voters in the locale. Each state has explicit requirements for voting machines, and, typically, each SBE or office of secretary of state will approve and certify equipment within a specified period of time before an election.

---

[6]Federal Election Commission (FEC), *Developing a Statewide Voter Registration Database: Procedures, Alternatives, and General Models* (Washington, D.C.: U.S. Gov't Printing Office, Autumn 1997),. 13.

A.3 Personnel

The SBE or secretary of state designates for each county a number of "election commissioners," who comprise the CBE, which typically appoints a Precinct Election Board (PEB) to administer and oversee election activities in each precinct within a county. A PEB usually consists of an inspector, or chairperson, and two judges drawn from the two major political parties (although, in some instances, the number of registered voters in a precinct may require the appointment of more judges). The CBE also appoints poll clerks and assistant poll clerks for each precinct. Precinct personnel usually are required to complete a training program and to take an oath of office.

A.4 Ballots

Every state provides the precincts within its jurisdiction with specifications for the format, printing, and distribution of sample and official ballots for all elections. Printing expenses are borne by the county treasury. State codes usually contain examples of paper ballots for primaries, general elections, and referendums as well as guidelines for voting machine ballots and ballot labels. The order of names and, if present, other items on the ballot should (as far as practicable) be identical with that on the paper ballots. Various codes specify other requirements for voting machine ballots, as indicated by this excerpt from the California Elections Code:

> The ballot label shall be printed by the elections official in black ink on clear material of a size that will fit the machine, of a color that may be determined by the elections official, and in as plain, clear type as the space will reasonably permit.[7]

Before a primary or an election, the CBE forwards sample ballots to every precinct and candidate on the ballot, to the chairperson of the county's central committee for each political party, to the newspapers, and, in some states, to all registered voters. The CBE determines the number of paper ballots or ballot labels, or both, required for the voting machines for each precinct, supervises the printing of the ballots, and distributes election materials and registration rolls to each precinct. Paper ballots are sequentially numbered and include stubs with spaces for the signature of the precinct election supervisor. For the sake of security and to control the potential for fraud, the number of paper ballots and ballot labels printed and distributed is recorded by the CBE, and the transportation of ballots to and from precincts is strictly controlled and supervised.

---

[7]California Elections Code, Div. 13, Ch. 3, Art. 5, Voting Machines, [On-line]. URL http://www.leginfo.ca.gov/.html/elec_table_of_contents.html (Accessed May 5, 2001.)

A.5 Candidates

The Constitution specifies criteria for the qualification of candidates for the offices of president, vice president, and for seats in the House of Representatives and the Senate. Because each state has its own criteria for candidates for state, county, and local offices, prospective qualified candidates for federal, state, and local offices have to follow numerous state-specific procedures for their names to be placed on a ballot for a primary or a general election. The Indiana state code, for example, specifies that "A person who desires to be nominated at a primary election as a candidate of a political party…for a federal, state, legislative, or local office shall file [with the secretary of state] a declaration of candidacy."[8] The declarations are reviewed and forwarded to the appropriate county circuit court judges, who publish the list of candidates.

Special state provisions usually apply to candidates for nomination to the office of the president in a primary election. For example, according to the Indiana Code, such candidates must file with the secretary of state "a written request that the candidate's name be placed upon the ballot under the label of the political party whose nomination the candidate is seeking."[9] This request must be accompanied by a petition signed by 5,000 voters in the state, including 500 in each congressional district. By contrast, in California the secretary of state can designate the names that appear on the primary ballot for each party.

A.6 Voter Authentication

Before entering a voting booth or completing a paper ballot at a poll site, eligible voters (also called electors) must sign a poll roster or the back of their registration cards and may also be required to produce verification of identity. Poll clerks or inspectors in each precinct maintain the roster and verify the eligibility of each prospective elector. The voter signs the registration book and the clerks compare the voter's signature with that on file. In some states, voters may be required to sign a receipt, which the verifying clerk then initials. Each voter then presents the receipt to a clerk staffing the voting booth or handing out printed ballots, and the clerk initials the receipt, places it in a sealed or locked container, and then permits the voter to vote. The receipt serves as "prima facie evidence that the person whose name appears thereon as an elector was admitted to the voting machine and that the person voted."[10]

A.7 Tabulation and Announcement of Results

After the polls close, every voting precinct is required to lock all voting machines and remove the seal from the boxes containing the ballots. The number of ballots cast is compared to

---

[8]Indiana Code §3-8-8-2, [On-line]. URL: http://www.state.in.us/legislative/ic/code/

[9]Ibid., Indiana Code §3-8-3-1.

[10]Florida State Code, Ch. 101,Voting Methods and Procedures, §101.47 (6), [On-line]. URL: http://election.dos.state.fl.us/fac/index.shtml

the number of voters on a list maintained by the precinct. If the numbers reconcile, the votes are counted. If they do not, then state-established procedures are used to rectify the discrepancy.

The votes for each candidate, as marked on paper ballots, displayed on mechanical counters, and on electronic printouts, are read aloud and counted. Absentee ballots are unsealed and counted. The number of unused or spoiled ballots is recorded. Each precinct produces a certificate of the results that lists the number of votes for each candidate on the ballot and the total number of votes for or against any referendum items. Electronic printouts of the tally are attached to the certificates. One copy of the certificate is sealed and transported to the CBE or county supervisor of elections for canvassing. Another copy is forwarded to a circuit court or county court judge. In both cases, the method of transport must adhere to strict guidelines. News media may be present at precincts to record the election results, which are then broadcast over local radio and television. The results may also be conveyed to the media by a designated PEB official.

A canvassing board (established by the county and typically comprising a county court judge and the chairperson of the county commissioners) examines in detail all certificates provided by the precincts. The board then makes and signs duplicate certificates certifying the total number of votes cast for each candidate for office (aggregated from the results from all the precincts), and the results are then conveyed to the media and may be placed on the Web sites of the county election office for public viewing. Posting results on Web sites has proved popular—so much so that some users could not access the county Web servers owing to overcrowding.[11]

All county certificates concerning the election of state or federal officers are transported to the SBE or the office of the secretary of state for verification. Some states also require a state canvassing board to review the election results. The SBE or secretary of state certifies to the governor the candidate receiving the highest number of votes for every office, except governor or lieutenant governor, and the results usually are forwarded to the state house of representatives. Certificates of Election are generated by the SBE, the secretary of state, or the governor, depending on specific office and state rules, and forwarded to the elected candidates. The election results are then communicated to the media and posted on state Web sites.

A.8 Procedures of the Electoral College

In a presidential election, the Electoral College, established by the Constitution, actually elects both the president and the vice president.[12] There are 538 presidential electors, drawn from

---

[11]FEC, Using the Internet in Election Offices (April 1998), 45, [On-line]. URL: http://www.federalregister.com/hpage/fesc.html (Accessed April 11, 2001.)

[12]"[T]he Electoral College system does not provide for residents of U.S. Territories, such as Puerto Rico, Guam, the U.S. Virgin Islands and U.S. Samoa to vote for President. Unless citizens in U.S. Territories have official residency (domicile) in a U.S. State or the District of Columbia (and vote by absentee ballot or travel to their State to vote), they cannot vote in the Presidential election." See "Can citizens in U.S. Territories vote for President?" Frequently Asked Questions on the Electoral College, prepared by the Office of the Federal Register, National Archives and Records

the 50 states and the District of Columbia, in an allotment equal to the number of members of the House of Representatives to which a state is entitled plus the 2 senators. The District of Columbia is allotted 3 electors "appointed by state-wide popular election."[13]

According to the National Archives and Records Administration's Procedural Guide to the Electoral College:

> [T]he Governor of each State and the Mayor of the District of Columbia prepare a Certificate of Ascertainment of the electors appointed (herein, the term "Governor" includes the Mayor of the District of Columbia). The Certificate of Ascertainment must list the names of the electors appointed and the number of votes received by each. It must also list the names of all other candidates for elector and the number of votes received by each. The Certificate must be signed by the Governor and carry the seal of the State. The format of the Certificate is not dictated by Federal law, but conforms to the law or custom of the submitting State.
>
> The Governor must prepare seven original Certificates of Ascertainment. One original, along with two authenticated copies (or two additional originals) must be sent by registered mail to the Archivist of the United States, National Archives and Records Administration…. The other six originals must be delivered to the State's electors….
>
> [T]he electors meet in their respective States [and] vote by ballot for President and Vice President…. The electors' votes are recorded on a Certificate of Vote…. One of the six Certificates of Ascertainment forwarded to the electors by the Governor must be attached to each of the six Certificates of Vote. Each of the six pairs of Certificates must be sealed and certified by the electors to be the list of votes of that State.
>
> The six pairs of Certificates are distributed as follows:
>
> – One, by registered mail, to the President of the United States Senate…;
>
> – Two, by registered mail, to the Archivist of the United States…;
>
> – Two to the Secretary of State of the State, one of which is held subject to the order of the President of the United States Senate, the other to be preserved by the Secretary for public inspection for one year; and
>
> – One to the chief judge of the Federal district court of the district in which the electors meet….[14]

Administration (NARA), [On-line]. URL: http://www.nara.gov/fedreg/elctcoll/faq.html - territories (Accessed July 3, 2001.)

[13]Office of the Federal Register, NARA, A Procedural Guide to the Electoral College, [On-line]. URL: http://www.nara.gov/fedreg/elctcoll/index.html (Accessed May 3, 2001.)

The official tally of the electoral votes takes place at a joint session of Congress in the House of Representatives, with the vice president as president of the Senate presiding and opening the sealed certificates so that the tellers can record the votes:

> The President of the Senate announces the results of the vote and declares which persons, if any, have been elected President and Vice President of the United States. The results are entered into the official journals of the House and Senate.[15]

The voting procedures of the Electoral College are not automated, and to date no effort has been made to diverge from the system established by the Constitution.

A.9 Absentee Registration and Voting

Every state has official rules regarding who can register to vote by absentee ballot. Typically, absentee registration and voting has been reserved for citizens covered under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) of 1986 as well as qualified voters, such as students, who will be absent from their county of residence on Election Day during poll hours. UOCAVA citizens use the Federal Post Card Application (also known as Federal Standard Form 76) to register to vote and request an absentee ballot. Citizens within the United States but are outside their home jurisdictions on Election Day may use the standard county registration form to register to vote, but they will also need to request an absentee ballot from the LEO using the standard form for that county.

Those wishing to vote by absentee ballot must complete an FPCA or a ballot request form and submit it by the deadline for that state. Once the form has been received at the LEO, it is validated and a note made in the registration files to send the citizen an absentee ballot. An absentee voter receives a blank ballot, completes it according to instructions, and signs it under oath (in some states, both filling out and signing the ballot must be witnessed by a notary public or other specified witness). Voters must mail the ballot to the county in a envelope with the printed return addressed of the county office and must sign their names across the seal of the envelope.

The county records the date each ballot is received and stores the ballots in a locked box in the county office. A canvassing board established by the county tabulates the absentee ballots within a period specified by the state. To protect against fraud and to ensure that all ballots are accounted for, the board usually compares the number of absentee ballots mailed to citizens to the number received by the LEO. The voters' signatures on the ballots are compared to signatures in

---

[14]Ibid.

[15]Ibid.; also, Ch. 1, 3 USC §15. See U.S. Code Electronic Edition, [On-line]. URL: http://www.access.gpo.gov/uscode/uscmain.html (Accessed July 3, 2001.)

the official registration books. Some counties use signature-retrieval systems to verify the signatures of absentee voters; the systems provide a digital image shown on a computer screen of a voter's signature which is compared to the voter's signature on the ballot, thus eliminating the need to search through paper files or use microfilm.[16] The digitized signature is scanned from the voter's signature on the registration document. An absentee ballot is considered invalid if the voter is not registered, if it is determined that the signatures do not match, if the ballot is not signed, or if all the required information is not provided. Absentee votes are tabulated and included in the total votes for the county. Once certified by the county, the votes are forwarded to the SBE or the secretary of state, depending on state law.

A.10 Referendums and Initiatives

The term "ballot proposal" is used here to mean "any constitutional amendment, proposition, referendum, or other question submitted to the voters at any election."[17] States that allow citizen-initiated ballot proposals (see **Figure A-1**) have codified requirements for the procedures. Typically, a group submits a draft proposal to the state attorney general for review. The attorney general prepares an official summary of the proposal to be used on petitions, which, sectioned by county, are then distributed. Each state specifies the number of signatures of eligible registered voters required on a petition for a proposal to be placed on a general election ballot. In California, two types of ballot initiatives can be placed on the ballot, and each requires a different percentage of signatures: a statute revision, which requires signatures equal to 5 percent of the total votes cast in the preceding gubernatorial election, and a constitutional amendment, which requires signatures equal to 8 percent of the total vote in the preceding gubernatorial election. If the required signatures are obtained, the petition is submitted to county election officials for signature verification. Some counties use signature-retrieval systems to verify the signatures (see section **A.9**). The petition is then forwarded to the secretary of state for review and submission to the legislature. The secretary of state furnishes the ballot title and the substance of every proposal to the supervisor of elections of every county.

The election processes outlined here may seem to have failed in the national election of 2000. Since then, governors across the country have been appointing task forces to examine ballot laws, legislative committees have begun preparations for hearings, and Congress has started to address proposals to improve the conduct of elections. At all levels—federal, state, and local—policymakers looking into reforms need to understand the present electoral process in detail for them to be able to examine Internet voting initiatives such as those discussed in **Appendix B**.

---

[16]Ralph C. Heikkila, *Election Signature Retrieval Systems*, edited by William C. Kimberling (Washington, D.C.: FEC, National Clearinghouse on Election Administration, 1992), 1.

[17]New York State Election Law, Article I, §101-4, [On-line]. URL: http://www.elections.state.ny.us/download/law/elaw.pdf (Accessed July 3, 2001.)

Source: ballot.org, Ballot Initiative Strategy Center, [On-line]. URL: http://www.ballot.org/states/index.html (Accessed July 3, 2001.)

Figure A-1

States That Allow Ballot Proposals

Appendix B

Internet Voting Initiatives

The possibilities of Internet technology, already on display in the speed of electronic transactions, appear particularly powerful and alluring in the aftermath of the presidential election of 2000. Public concern that the nation's highest officials may be selected with the use of outdated voting machines has led to calls for the development of a modern voting infrastructure based on "cutting edge" information technologies. As shown by the following review of major initiatives in the public and private sectors, even before the problems associated with the national election of 2000 came to light, efforts to study and experiment with Internet voting had been under way.

B.1 Trial Elections at Universities, Colleges, and High Schools

In 1999 and 2000, college and high school students across the United States participated in mock elections, including presidential preference primaries, and in binding student government elections conducted over the Internet. Many of the mock elections incorporated up-to-date on-line voting in which students were not restricted to voting at polling sites but could vote from home, work, or a library—any location with access to the Internet.[1] For example, over two days, March 6–8, 2000, students at Kansas State University participated in a binding election over the Internet to elect officials to the student governing association. And on March 14, before the Florida Democratic and Republican primaries more than five thousand high school students in that state cast mock, nonbinding votes in a presidential primary conducted over the Internet.

B.2 The California Internet Voting Task Force

With its long history as a leader in election reform and in referendum politics, California, to no one's surprise, has been in the vanguard of those considering voting over the Internet. In response to grassroots pressure to consider Internet voting as an alternative to traditional voting, California established a task force of state officials, academics, and leaders from the information technology industries to study the feasibility of using the Internet to conduct elections. The task force was charged with identifying and exploring the issues raised by Internet voting and with recommending an appropriate timeline for introducing Internet technologies into the California electoral process. The report issued by the task force—the most important work to date on Internet voting—suggested that Internet-based registration and voting may increase access to the

[1]See URL: http://www.votehere.net/elections.html (Accessed May 13, 2001.)

voting process for millions of citizens who do not regularly participate in traditional elections.[2] The task force concluded, however, that until the potential for threats to the security, integrity, and privacy of Internet-based registration and voting has been addressed, the prudent approach would be to include Internet voting in the electoral process in four stages:[3]

Stage 1: Introduce Internet voting machines at traditional polling places and allow voters to select either an Internet or a paper ballot;

Stage 2: Allow voters to cast ballots on any county-controlled Internet voting machine as long as election officials are present to ensure voter authentication;

Stage 3: Provide voter authentication codes that allow voters to cast a ballot at any unattended county-controlled Internet voting machine; and

Stage 4: Provide voter authentication codes that allow voters to cast ballots from a home or office computer.

In addition, the task force offered two key contributions to the debate on Internet voting. First, it distinguished between the processes of registering to vote and the actual casting of ballots. In particular, it noted the difficulty in an Internet-based system of identifying and authenticating voters:

> A comprehensive Internet-based election system would require the use of a universally available form of digital identification that would allow election officials to verify both the identity and eligibility of potential voters. Although the technology is capable of creating a universal digital identification system, that form of identification is not readily available and accessible to all voters…. In the absence of digital identification, Internet-based voter registration is not secure.[4]

Second, the task force described the following threats and challenges unique to an Internet-based system that are not considered serious dangers to election systems in the present configuration and not dealt with by present election procedures and regulations:

- **Voter authentication:** Determination that a ballot that arrives at the "vote server" is from the registered voter it purports to be from.
- **Privacy of the ballot:** Preservation of the secrecy of the ballot so that no unauthorized person can read the ballot and no one can associate it with the voter who cast it.

---

[2]Office of the Secretary of State, California Internet Voting Task Force, Brief History of Voting Systems, in The Internet Voting Report, Jan.18, 2000, [On-line]. URL: http://www.ss.ca.gov/executive/ivote/final_report.htm#final-1 (Accessed March 17, 2000.)

[3]Ibid., 15.

[4]Ibid.

- **Ballot integrity:** The guarantee that ballots cannot be changed surreptitiously by any software agent or trusted third party.
- **Reliable transport and storage of ballots:** The guarantee that no ballot is either created or destroyed (lost) anywhere between the "vote client" and "vote server" without detection, and that no ballots are created or destroyed (lost) between vote servers and vote canvas computers.
- **Prevention of "multiple voting":** That no more than one ballot may be counted for any one voter.
- **Defense against malicious software:** The guarantee that no malicious software (Trojan horse, virus, etc.) that could affect the integrity or privacy of the ballot will be on the client-server of election officials or on voters' computers.
- **Defense against denial-of-service attacks:** That deliberate attacks intended to control, crash, or overload computers and networks that support election officials or voters or both will be dealt with.[5]

In the months after the task force issued its report, California continued to consider Internet voting options. For example, on Election Day it conducted four "trials" of Internet voting in which voters cast mock ballots. Although the votes in these trials were not binding in the national election, the trials could be used to assess voters' interest in Internet voting as an alternative to traditional voting procedures.

B.3 The Alaska Straw Poll

On January 24, 2000, VoteHere.net became the first company to conduct a public Internet election when Alaskans in three northern districts, as well as the state's congressional delegation, voted over the Internet in a Republican presidential straw poll.[6] In total, thirty-five out of fifty-six eligible registered Republican voters took part, voting from home, a public location, or a public polling station. According to Thomas McKay, chairman of the Alaska Republican Party, "There has been a high level of interest and excitement over this project. Many people in the bush feel neglected, and we are trying to counter that perception by using this breakthrough technology to bring democracy to their doorsteps. Due to natural barriers, it has been difficult for these U.S. citizens to participate in the democratic process."[7] Members of the straw poll committee

---

[5]In addition to its study of the legal, policy, and procedural issues associated with Internet voting, the California Internet Voting Task Force produced a technical appendix that examined technology-specific issues; see URL: http://www.ss.ca.gov/executive/ivote/appendix_a6.htm (Accessed March 13, 2000.)

[6]Press release, VoteHere.net, "VoteHere.net Conducts First Binding Internet Election; Alaska Republicans Vote Online in Party Straw Poll," Jan. 26, 2000, [On-line]. URL: http://www.votehere.net/news/archive00/012600.html (Accessed July 3, 2001.)

[7]Press Release, VoteHere.net, "VoteHere.net to Conduct First Binding Internet Election," Dec. 10, 1999, [On-line]. URL: http://www.votehere.net/news/archive99/121099.html (Accessed July 3, 2001.)

concurred, confident that Internet voting would encourage more Alaskans to vote by alleviating such deterrents as vast distances, lack of transportation, and unreliable postal service.

In the system VoteHere.net deployed in Alaska, ballots were encrypted and stored in a secure server; for the straw poll, in each ballot the voter's name was followed by an encrypted string of alphanumeric characters for each vote the voter cast.[8] According to VoteHere.net, this ensured that the ballots showed *who* voted, but not *how* they voted, thereby protecting the privacy of the ballot.[9]

B.4 The Arizona Democratic Primary

In March of 2000, Arizona's Democratic Party participated in the first binding, statewide partially Internet-based primary election, in which approximately forty thousand registered Democrats cast electronic ballots. The Internet-based portion was managed and executed by election.com, a private company.[10]

The process was as follows: election.com mailed PINs to every registered Democratic voter in the state. Interested voters accessed election.com's Web site and entered their PIN numbers. Voters were prompted to answer several personal questions, and the answers were then compared to information on the their registration cards. After authentication, a ballot appeared on screen. Voters selected their choice and submitted their votes. Voters could cast electronic ballots up to five days before the primary. Emphasizing the security features of its Web site, election.com stated that it used "state-of-the-art SSL [secure socket layer] encryption to secure Internet elections" and that its server was "authenticated through a Secure Server ID [that] protects against hacking and program tampering."[11] Information on whether and how voters' computers may have been secured was not available, and the precise security precautions and architecture used remain election.com's closely held secret.

Arizona's Democratic primary raised the issue of the economic and social "digital divide" and its implications for Internet-based elections in the future. According to a lawsuit the Voting Integrity Project filed in Phoenix the month of the primary on behalf of four Arizona Democrats,

> Internet voting violates the Voting Rights Act because it provides voting opportunities to some voters but not to all voters. Specifically, the Arizona Democratic Party plan increases the strength of white voters, who on

---

[8]See URL: http://www.votehere.net/content/Products.asp

[9]Ibid.

[10]James Ledbetter, "Arizona Democrats, Online Voting," The Industry Standard Magazine (March 10, 2000), [On-line]. URL: http://www.thestandard.com/article/0,1902,12858,00.html (Accessed April 24, 2001.) See, also, "The Red Herring 100 Company Profiles," *The Red Herring* **79** (June 2000), 144, 356.

[11]See URL: http://www.election.com/

> balance have greater access to the Internet, at the expense of African-American, Hispanic, and Native U.S. voters, who on balance have less access to the Internet.[12]

The suit contended that the "Internet voting system planned for the Arizona Democratic Presidential Primary will have the effect of maximizing affluent white participation relative to non-whites in the primary."[13] The presiding judge was quoted as recognizing that Internet voting may "result in racial discrimination in this election," but let the election take place, stating that the results could be discarded if it were determined that Internet voting significantly skewed voter demographics.[14]

Owing to the sheer size of the participating population and the variety of the voting channels used (in addition to voting over the Internet, voters could vote by postal mail and telephone), the Arizona Democratic primary is being widely studied.[15]

B.5 National Party Conventions

In 2000, the Democratic, Republican, and Reform parties all considered limited experiments with on-line voting at their convention sites. At the Democratic national convention (August 16–19), a variety of information technologies were used to conduct the first "e-Convention," in which delegates used technology provided by election.com to "cast their nomination votes for Al Gore."[16] Smart-card technology was used to provide delegates with access to convention facilities and such services as program updates and to purchase food and beverages. For the Republican convention (July 31 to August 3), VoteHere.net was selected to supply an on-line voting system "to collect and tabulate platform votes from the floor,"[17] although, in the end, the system was not used. For the Reform Party convention (August 10–13), eBallot was selected to allow party members to "cast their ballot[s] for the party's presidential

---

[12]Press release, Voting Integrity Project, "VIP Will Not Appeal Judge's Decision Allowing Internet Primary to Proceed but Will Fight Onward with Voting Rights Act Claim," March 3, 2000, [On-line]. URL: http://www.voting-integrity.org/text/2000/rel030300.htm (Accessed March 17, 2000.)

[13]Ibid.

[14]Ibid.

[15]For a study that examines the Arizona Democratic primary, see R. Michael Alvarez and Jonathan Nagler, "The Likely Consequences of Internet Voting for Political Representation" (Sept. 19, 2000), [On-line]. URL: http://www.netvoting.org/resources.htm (Accessed Oct. 12, 2000.)

[16]Press release, election.com, "election.com Places 2000 Democratic National Convention in the History Books as the First Successful e-Convention," Sept. 7, 2000, [On-line]. URL: http://www.election.com/ (Accessed May 13, 2001.)

[17]Press release, VoteHere.net, "VoteHere.net Brings Online Voting Technology to Republican National Convention," July 31, 2000.

nominee…during a brief period"[18] over the Internet and by telephone. The tumult surrounding the nomination of Patrick Buchanan, however, and sharp divisions within the Reform Party complicated efforts to deploy and test the system.

B.6 The National Science Foundation

On October 11–12, 2000, the NSF, in conjunction with the Internet Policy Institute,[19] sponsored a symposium on Internet voting at the Freedom Forum in Washington, D.C.,[20] which brought together technologists, including computer security experts, and social scientists, election officials, and archivists, to consider the implications of Internet voting, identify critical issues in on-line voting, define an agenda for future research, and produce a report with recommendations. The topics discussed at the symposium included the following:

- how to ensure the security and reliability of the voting process;
- how to protect the privacy of voters;
- how to authenticate voter identity;
- how to achieve broad and equitable access to on-line voting systems;
- how to assess the impact of on-line voting on representative democracy and community; and
- how to ensure that on-line voting systems are convenient, flexible, and cost effective.[21]

On March 6, 2001, the NSF and the Internet Policy Institute issued their Report on the National Workshop on Internet Voting: Issues and Research Agenda, which described the technical and social science issues related to Internet voting and suggested a R&D roadmap to address them.[22]

B.7 The ICANN Election

In October of 2000, the Internet Corporation for Assigned Names and Numbers partnered with election.com to allow its at-large members to vote over the Internet to select five new directors of the corporation. More than 75,000 members over the age of sixteen attempted to

---

[18]"Reform Party to Use Internet Voting," *The Washington Post*, June 12, 2000, A-7.

[19]According to its Web site, the Internet Policy Institute is "the nation's first independent, nonprofit research, and educational institute created to provide objective, high-quality analysis, research, education, and outreach on public policy issues affecting and affected by the global development and use of the Internet." See URL: http://www.internetpolicy.org/ (Accessed April 12, 2001.)

[20]Internet Policy Institute, "National Workshop on Internet Voting," sponsored by the NSF, conducted in cooperation with the University of Maryland, and hosted by the Freedom Forum, Oct. 11–12, 2000, [On-line]. URL: http://www.netvoting.org/ (Accessed April 12, 2001.)

[21]Ibid.

[22]Ibid., see Report on the National Workshop on Internet Voting: Issues and Research Agenda, (March 6, 2000).

participate and cast on-line ballots, but in several circumstances programming glitches resulted in error messages and, thus, complaints about the difficulties encountered.[23]

B.8 The Federal Voting Assistance Program

In November of 2000, a pilot project called Voting Over the Internet (VOI), managed by the FVAP, extended Internet voting to approximately ninety voters covered under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) (1986). Housed within the Department of Defense, the FVAP has the following mission:

- to inform and educate u.s. citizens worldwide of their right to vote;
- to foster voting participation; and
- to protect the integrity of, and to enhance, the electoral process at the federal, state, and local levels. [24]

Consistent with that mission, in 1999 the FVAP began a small Internet voting pilot project "primarily aimed at making it easier for service members stationed away from their home states to cast their ballots."[25] Participants included out-of-state and overseas military personnel, their families, and other U.S. citizens living abroad and therefore not at their voting precincts during polling hours on Election Day. Counties in Florida, South Carolina, Utah, and Texas volunteered to take part in the pilot project.[26]

The VOI project's pilot system was designed to function as a registration and ballot-delivery system that directly replicated mail-in absentee ballot procedures used by local election officials in the participating jurisdictions.[27] Citizens registered on line, requested an absentee ballot, and voted on Election Day by using a public-key infrastructure certificate to authenticate personal identity. The system was not designed to tabulate votes, and local elections officials

---

[23]James Evans, "ICANN Election Starts with Small Snag," Network World Fusion News, Oct. 2, 2000, [On-line]. URL: http://www.nwfusion.com/news/2000/1002icann.html (Accessed April 25, 2001.)

[24]For the program's mission and goals, see the home page of the FVAP at URL: http://www.fvap.ncr.gov/fvap.html (Accessed July 10, 2001.)

[25]Paul Stone, "DOD to Test Online Absentee Voting," U.S. Forces Press Service (June 25, 1999), [On-line]. URL: http://www.defenselink.mil/news/Jun1999/n06251999_9906252.html (Accessed July 23, 2001.)

[26]Participating counties were Okaloosa County and Orange County, Florida; all counties in South Carolina; Weber County, Utah; and Dallas County, Texas.

[27]Testimony of David O. Cooke, director, administration and management office of the Secretary of Defense, at a hearing before the U.S. House of Representatives Military Personnel Subcommittee on May 9, 2001, [On-line]. URL: http://www.house.gov/hasc/openingstatementsandpressreleases/107thcongress/01-05-09cooke.html (Accessed May 13, 2001.) See also: William Matthews, "Election Day Winner: Online Voting," *Federal Computer Week* (Nov. 10, 2000), [On-line]. URL: http://www.fcw.com/fcw/articles/2000/1106/web-elect-11-10-00.asp (Accessed Nov. 17, 2000.); and Jim Garamone, "Say Goodbye to Chad, DoD Tests Internet Voting," U.S. Forces Press Service, Jan. 25, 2001, [On-line]. URL: http://www.defenselink.mil/news/Jan2001/n01252001_200101254.html (Accessed April 25, 2001.).

remained responsible for transposing absentee ballots submitted on the Internet into traditional forms that were counted along with other absentee ballots by the locality's tabulating machines.

The VOI system, an experiment in on-line registration and voting, in using digital certificates to identify citizens and in allowing remote voting from the home or office, was significant in three respects. First, given the circumstance in which votes were submitted, it closely correlates with Stage 4 proposed by the California Internet Voting Task Force. Second, participants submitted binding absentee votes over the Internet in a national election from locations as distant as Korea and Saudi Arabia. That is, unlike the primaries in Arizona and Alaska, in which the standards and regulations were less stringent, the VOI system was required to comply with federal, state, and local election laws, regulations, and procedures. Third, unlike systems used in the primaries in Alaska and Arizona, the VOI system was applied in several states and localities.

B.9 Trial Elections in California and Arizona

As leaders in the Internet voting field, California and Arizona conducted independent experiments in 2000 using Internet-based voting in trial elections. In Arizona, VoteHere.net was contracted to conduct a pilot program to "give voters an opportunity to vote a sample ballot using the latest online technology."[28] It was designed to meet the state of Arizona's criteria for ensuring the integrity of the election and—important to voters—a secure and private ballot.[29]

California sponsored four demonstration elections in four counties—Contra Costa, Sacramento, San Diego, and San Mateo—where "[v]oters were able to cast non-binding ballots from online voting machines in central locations."[30] To enhance the demonstrations, California selected three vendors to test different technological solutions—VoteHere.net for Sacramento and San Diego counties, Safevote.com for Contra Costa County; and Election Systems and Software in San Mateo County.

---

[28]Press release, Betsey Bayless, Secretary of State, Arizona, "Secretary Bayless and Recorder Purcell to Conduct Election Day Online Voting Trial," [On-line]. URL: http://www.sosaz.com/release/pressrelease55.htm (Accessed on Dec. 12, 2001.)

[29]Ibid.

[30]According to the Web site "Online Voting Demonstrations" of the Secretary of State of California, Bill Jones, "Voters were able to cast non-binding ballots from online voting machines in central locations in the counties of Contra Costa, Sacramento, San Diego, and San Mateo," [On-line]. URL: http://www.ss.ca.gov/elections/elections_online_demo.htm (Accessed July 30, 2001.)

B.10 Election Reform Initiatives

Several election reform initiatives were launched within weeks after resolution of the presidential election of 2000.[31] The problems and shortcomings in the tally of the presidential vote in Florida led Governor Jeb Bush to create a task force to examine election procedures, standards, and technology. On March 1, 2001, the task force issued its report.[32] Similar initiatives to examine voting technologies and processes were launched in Maryland and Georgia. In February of 2001, the National Association of Secretaries of State (NASS) initiated an examination of the issues facing the states,[33] and a National Commission on Federal Election Reform, co-chaired by former presidents Gerald Ford and Jimmy Carter, was organized to recommend ways to improve the accuracy and fairness of federal elections.[34]

Congress, too, has taken a keen interest in election technologies and procedures. In particular, the 107th Congress has begun to address two major problems, the election infrastructure and the issue of equal access. The present election infrastructure is generally regarded as dependent on antiquated technology ill-suited to the information age. As of May of 2001, several bills had been sponsored and hearings conducted in both the Senate and the House. Senators Mitch McConnell (Rep.-Ky.), Charles E. Schumer (Dem.-N.Y.), John McCain (Rep.-Ariz.), and William Nelson (Rep.-Fla.) had sponsored bills to address various aspects of election reform, technology, and modernization.[35] The election of 2000 revealed that minority voters and voters with low incomes nationally, and in particular in Florida and New Jersey, among other states, have been forced to vote on old machines and to wait at polling places for a long time and in long

---

[31]For a list of recent developments in election reform, see The Brookings Institution's list of "essential cases, legal and policy materials, and legislative developments on election reform," [On-line]. URL: http://www.brookings.org/GS/Projects/ElectionReform.htm (Accessed May 7, 2001.)

[32]Revitalizing Democracy in Florida: the Governor's Select Task Force on Election Procedures and Technology, March 1, 2001, [On-line]. URL: http://www.brook.edu/gs/research/electionreform.htm (Accessed June 18, 2001.)

[33]For NASS's resolution on election reform and associated white papers, see URL: http://www.nass.org (Accessed Aug. 1, 2001.)

[34]See URL: http://www.reformelections.org

[35]Election reform bills proposed include the following: Senator McConnell introduced S. 218, "The Election Reform Act of 2001," which was, among other things, intended to establish an Election Administration Commission to consider issues related to election technology and ballot design, access to polling places, voter registration and verification, alternative voting methods, and the accuracy and security of election procedures and vote counts. This bill was combined with H.R. 263, the House companion piece of legislation introduced by Representative Tom Davis (Rep.-Va.), "The Election Reform Act of 2001" and a bill proposed by Senator Schumer, S. 379, "The Election Modernization Act of 2001," to establish a national commission to study current and alternate voting methods and issues involving voter accessibility, federal election administration, and federal assistance to state and local authorities to improve such administration. Senator McCain proposed an election reform bill, S. 368, "U.S. Voting Standards and Technology Act of 2001," that would adopt a more technology-centric approach and vest authority in the National Institute of Standards and Technology to examine technology issues and develop voluntary election standards for equipment. Senator Nelson sponsored S. 729, "The Internet Voting Expansion Act of 2001," which would authorize the attorney general to award grants to states to enable them to expand opportunities for citizens to vote over the Internet.

lines, and their votes often have been disproportionately disqualified. Owing to these problems, the issue of equal access has drawn wide attention, and, as of May of 2001, at least one bill had been introduced in the Senate, by Christopher Dodd (Dem.-Conn.), that seeks to address the problems of access by creating federal grants and oversight under the Department of Justice.[36]

[36]S. 565, "Equal Protection of Voting Rights Act of 2001," would establish a Commission on Voting Rights and Procedures to study election technology, voting, and election administration and establish a program of grants to develop uniform, nondiscriminatory requirements for election technology and administration.

Appendix C

Other Activities Related to Internet Voting

This appendix summarizes major studies, reports, and other on-line voting activities related, directly or indirectly, to Internet voting.

C.1 Studies of the "Digital Divide"

In the 1990s, the National Telecommunications and Information Administration conducted surveys that culminated in a series of studies of the digital divide: *Falling Through the Net: A Survey of the "Have Nots" in Rural and Urban America* (July 1995); *Falling Through the Net II: New Data on the Digital Divide* (1997); and *Falling Through the Net III: Defining the Digital Divide* (1999) (see section **3.1**).[1]

On December 9, 1999, President Clinton announced several initiatives, including the request to the NSF to offer grants for research into issues of digital government, including the "digital divide" and Internet voting (see section **3.2**).[2] Over the next year and a half, several studies continued the national debate on the digital divide, most notably one published by Stanford University that "debunked" the statistics used to support evidence of a digital divide.[3]

C.2 The Democracy Online Project

In October of 1998, the Pew Charitable Trusts funded a grant to the Graduate School of Political Management at George Washington University, in Washington, D.C., to form the Democracy Online Project, which promotes the development of U.S. on-line politics "in a manner that will uphold democratic principles and values."[4] The project conducts research on on-line politics, focusing on U.S. campaigns and elections, the promotion of standards for the conduct of on-line campaigning, and the creation and promotion of on-line public space. As part of the research, the project has sponsored a series of sessions of public testimony.

---

[1]NTIA, U.S. Dept. of Commerce, [On-line]. URL: http://www.ntia.doc.gov/ntiahome/net2/falling.html (Accessed Sept. 13, 2000.)

[2]Remarks by President William J. Clinton, Bridging the Digital Divide, The White House, Dec. 9, 1999, [On-line]. URL: http://clinton6.nara.gov/1999/12/1999-12-09-remarks-by-the-president-on-bridging-the-digital-divide.html (Accessed June 13, 2001.)

[3]Roger G. Noll, Dina Older-Aguilar, Gregory L. Rosston, and Richard R. Ross, in *The Digital Divide: Definitions, Measurement, and Policy Issues* (Stanford University) indicate factors other than income (e.g., level of education) that may explain the digital divide. See URL: http://www.ccst.ucr.edu/cpa/bdd/BDDreport/BDD05.html (Accessed Aug. 10, 2001.)

[4]Democracy Online Project, "Project Overview," [On-line]. URL: http://www.democracyonline.org (Accessed Feb. 17, 2000.)

C.3 The "Future of Internet Voting" Symposium

The Brookings Institution, in collaboration with Cisco Systems, Inc., began to explore Internet voting at a symposium on "The Future of Internet Voting," held on January 20, 2000, in Washington, D.C. The symposium was the first of a projected series on "how the Internet might affect democracy and governance in the twenty-first century."[5] Panelists addressed pilot projects, "technical hurdles of ensuring security and privacy," concerns about "disparate access to voting systems," and the possible impact of Internet voting on voter turnout, as well as the "broader implications of the digital revolution for representative democracy."

C.4 The Voting Integrity Project

Founded in 1996, the Voting Integrity Project is a national, nonpartisan voters' rights organization dedicated to protecting free elections in the United States.[6] It has developed several programs on poll watching, monitoring, and registration intended to educate voters about their rights and to ensure that elections will be conducted with the highest degree of integrity. In 1999, the VIP entered the public debate on Internet voting with its study "Are We Ready for Internet Voting?" which examined the new threats to voters' rights and to the integrity of elections posed by on-line voting and which concluded that these threats were still too great to move forward with Internet voting (see section **4.2**).[7] In March of 2000, the VIP filed a lawsuit on behalf of minority voters, challenging the Arizona Democratic party's plan to allow on-line voting in its presidential primary.

C.5 Elections in Other Countries

Foreign experiments with Internet voting as a solution to such problems as poor voter turnout and the high costs of voting have met with mixed results. Since the mid-1990s, several international initiatives have demonstrated a growing interest in Internet voting. Among the countries that have either conducted or contemplated some form of Internet-based voting are France, Costa Rica, and Bosnia, with results described below, as well as Croatia, the United Kingdom, South Africa, and Venezuela. Some experiments were implemented successfully, while some ambitious attempts confronted obstacles that seemed difficult to overcome. Information on these initiatives remains largely anecdotal, because no formal pilot study or evaluation was conducted. The three experiments described here provide only a "snapshot" of international efforts and are not intended to be exhaustive.

---

[5]See URL: http://www.brookings.org/ (Accessed April 12, 2001.)

[6]Voting Integrity Project, URL: http://www.voting-integrity.org/ (Accessed May 11, 2001.)

[7]Deborah M Phillips, "Are We Ready for Internet Voting?" Voting Integrity Project" (Aug. 12, 1999), [On-line]. URL: http://www.voting-integrity.org/projects/votingtechnology/internetvoting/ivp_title.shtml (Accessed April 12, 2001.)

The first occurred in the final week of September of 2000. Voters in Brest, France, used on-line voting technologies to "cast their opinions in the country's first government-organized online referendum."[8] The project was viewed as a local pilot that might see broader application across France, which makes extensive use of national, regional, and local plebiscites and referendums.

The second, an Internet-based voting initiative proposed in 1997 in Costa Rica, was aimed at increasing electoral participation and efficiency while reducing the costs of the election process. Because citizens in that country are reluctant to register to vote anywhere other than where they originally registered at the age of eighteen, political parties spend the equivalent of millions of dollars every election year to bus voters to polling stations or to give them money for gas to use to go to registration locations.[9] Given that Costa Rica's telecommunications infrastructure is more advanced than in many other countries in Latin America, the Supreme Electoral Tribunal of Costa Rica believed that national elections could be held on the Internet at polling stations located in public schools. This would allow voters to vote anywhere in the country.

On February 1, 1997, Project Costa Rica, developed by the Center for Information Law and Policy, with students from the Villanova University School of Law, in Pennsylvania, and the Illinois Institute of Technology's Chicago–Kent College of Law, as well as researchers from the AT&T Research Laboratories and the government of Costa Rica, was to have been the country's first test of a national on-line election. According to Brett Amdur, director of technology at the Center for Information Law and Policy, the project would have demonstrated that electronic elections could be conducted securely on a broad scale.[10] Had it succeeded, the government planned to discontinue the use of paper ballots and rely entirely on the Internet for the national election of 2002. Some weeks before the election, however, for reasons unknown to the leaders of Project Costa Rica, the government of Costa Rica decided to postpone the test.

The third experiment was an Internet-based election in Bosnia proposed by the Center for Information Law and Policy to the Organization for Security and Co-operation in Europe (OSCE), in an effort to achieve free and fair elections.[11] Safe access to polling locations was a particularly important issue in encouraging a high voter turnout. The OSCE's team felt that voting over the Internet would allow participants to vote from outside the municipalities where they had formerly lived, thereby reducing the administrative costs of protecting voters returning to those

---

[8]Press release, election.com, "election.com Conducts Online Referendum in City of Brest, France," Oct. 4, 2000, [On-line]. URL: http://www.election.com/us/pressroom/pr2000/1004.htm (Accessed April 12, 2001.)

[9]Jeri Clausing, "Costa Rica to Try Online Elections," *The New York Times*, Oct. 22, 1997, [On-line]. URL: http://www.nytimes.com/library/cyber/week/102297costarica.html

[10]Ibid.

[11]International Institute for Democracy and Electoral Assistance, The Internet and the Electoral Process, [On-line]. URL: http://www.idea.int/publications/techintro.html (Accessed Nov. 17, 1999.)

areas.[12] The team argued that an Internet-based election could be made sufficiently secure to ensure the integrity of the election. Although the OSCE considered the project, it ultimately abandoned the idea.

C.6 Proxy Voting

In the United States, technology has begun to revolutionize how corporate shareholders vote proxies. Electronic proxy voting by telephone and over the Internet is relatively new and cost efficient; it allows companies incorporated in certain states to provide a convenience to shareholders.[13] Companies that offer these services can tally votes quickly and thereby significantly reduce the costs associated with traditional paper-based proxies. Some experts, such as Carl Hagberg of Carl T. Hagberg & Associates, believe that Internet proxy voting may become part of corporate marketing, investor relations, and e-commerce strategies, helping shareholders to become increasingly accustomed to accepting electronic goods and services from companies.[14]

Although proxy voting by telephone is still more frequent than Internet voting, according to a survey conducted in April of 1999 by Investor Relations Business, both forms of electronic proxy voting are on the rise, from use by approximately 40 firms in 1997 to by almost 150 in 1998, for a 300 percent increase in a year.[15] Shareholders from 1,000 to several million were provided with electronic proxies in addition to traditional paper proxies. Internet voting is expected to expand as more companies and shareholders use it for business operations and financial transactions. According to Richard Vancil, then former senior vice president of Shareholder.com (previously the Direct Report Corporation), "In a survey of 2.4 million votes by registered shareholders from 35 clients of transfer agent Boston Equiserve, 500,000, or 20%, were voted electronically during the March to May 1998 proxy season…85% of the electronic votes were via telephone, and 15% were over the Internet."[16]

Initially, Internet-based proxy voting was similar to proxy voting by telephone in that shareholders received by postal mail a proxy package with a printed annual report[17] and a proxy statement with a Web address (uniform resource locator [URL]) and a PIN. The shareholder was

---

[12]Ibid.

[13]Charles J. Purcer, "Electronic Voting About to Explode," StockTransfer.com, April 4, 1998, [On-line]. URL: http://www.stocktransfer.com/investorrelations.htm#electronic-voting-about-to-explode (Accessed April 23, 2001.)

[14]Elizabeth Judd, "eVoting 2000," IR Magazine (1999), [On-line] URL: http://www.irmag.com/feature.asp?articleID=815 (Accessed Aug. 24, 2001.)

[15]Investor Relations Business, "Electronic Proxy Voting May Double This Year" (April 1999), [On-line]. URL: http://www.shareholder.com/home/issues/proxy.cfm (Accessed Nov. 27, 1999.)

[16]Interview with Richard Vancil, by David Svec, Joseph Butcher, Katie Hines, and Erin MacDougall, Jan. 12, 2000.

[17]Ronald H. Gruner, "Electronic Proxy Voting: 'The Best Is Yet to Come,'" U.S. Society of Corporate Secretaries Summer 1998 Newsletter, [On-line]. URL: http://www.shareholder.com/home_june8/issues/electronic.cfm (Accessed Dec. 28, 1999.)

connected with the Web site and guided through the voting process, typically requiring only a few minutes.[18] After a vote was cast, most proxy voting systems e-mailed the stockholder confirmation of the vote.

Firms such as Microsoft and Intel are allowed, by U.S. Securities and Exchange Commission Release Numbers 33-7233 and 33-7288, to take another approach to proxy voting over the Internet.[19] These companies e-mail proxy notices to interested shareholders, who can find the information they need to decide their views posted on the companies' Web sites.[20] Voting over the Internet saves companies both time and money by eliminating the costs of preparing and mailing printed proxies. A totally Internet-based system, in which proxy statements and annual reports would be available on-line, has been estimated to save as much as $5.00 per shareholder by eliminating the costs of printing and mailing and by reducing tabulation costs by 80 to 90 percent, that is, to less than 10 cents per vote.[21]

Information security has not appeared to be an important issue for either the proxy voters or the investor relations departments of public companies. According to Shareholder.com, among others, the voting systems of investor services companies are both redundant and secure.[22] The security of individual votes is maintained by control numbers in which "control digits" are embedded that are then validated against a set of ranges and mathematical algorithms before voters have access to the system. Internet-based voting enables the companies' clients to capture real-time voting statistics conveniently. The one minor drawback to Internet proxy voting has been the occasionally slow response of the Web that some investors experience when network traffic increases during voting.[23]

Internet proxy voting has proved a viable option for many corporations. Theoretically, the Internet promises to lower the costs of proxy voting for corporations as well as allow them to be regarded as progressive because they provide on-line business services. The cost savings materialize, however, only after a significant number of shareholders use the Internet-based voting systems.[24] As high-performance information systems come to be used increasingly in the United States, slow, unresponsive, or unreliable voting systems might lead stockholders to a negative view of a company. These factors will need to be considered by investor relations managers making decisions on whether to use the Internet as a voting tool.

---

[18]Ibid.

[19]"Sending Proxies and Annual Reports via the Internet," [On-line]. StockTransfer.com, [On-line]. URL: http://www.stocktransfer.com/investorrelations.htm (Accessed Jan. 20, 2000.)

[20]Gruner, "Electronic Proxy Voting."

[21]Ibid.

[22]Interview with Richard Vancil.

[23]Gruner.

[24]Elizabeth Judd, "eVoting 2000."

C.7 Labor Union Elections

Labor unions have been experimenting with Internet voting technologies and on-line voting and polling. In June of 2000, the Boeing Company and the Society of Professional Engineering Employees in Aerospace (SPEEA), which represents more than 22,000 engineers and technical workers, used Internet voting to settle a labor dispute.[25] After forty days of negotiations for a new labor contract,[26] the dispute was resolved in a vote over the Internet in which more than 70 percent of the SPEEA members voted to accept the contract.[27] By conducting the vote over the Internet, both parties to the dispute avoided the slower, conventional mail-in vote and decisions were made more quickly than previously. Out-of-area SPEEA members, instead of sending ballots through the postal system, had access to the computer voting system and cast ballots along with on-site members. Thus, in this instance, Internet voting, with its quick balloting and tallying of votes, usefully replaced mailed ballots and facilitated the resolution of a dispute.

C.8 The Web and Political Discourse

Although a full discussion of the effect of the Web and of related technologies on political discourse in the United States and elsewhere is beyond the scope of this report, it is clear that many aspects of politics, campaigning, and elections are being transformed from the physical to the immaterial in cyberspace. Candidates are using the Internet to raise funds, mobilize supporters, and inform the electorate about their positions. The FEC has handed down a series of decisions governing the Internet for fundraising.[28] The decisions comment on candidates' official Web sites and "fan sites," with different rules governing fan sites that support a candidate without the candidate's approval from those for sites coordinated with a candidate's official efforts.

The emergence of dot-com and dot-org Web sites dedicated to providing information on candidates and political issues has had an effect on public discourse. Founded in 1999 to capitalize on the emerging market built on politics and the Internet, grassroots.com and selectsmart.com provide the technical means with which groups can mobilize a popular movement: they create and run programs to organize groups and send mass e-mail messages to politicians. Experts predict that, because members of Congress are now alert to professional e-mail organizers and can simply delete their messages and choose instead to read only unique

---

[25]See press release, VoteHere.net, "Internet Voting Technology Facilitates Rapid Resolution of SPEEA-Boeing Contract Dispute," March 19, 2000, [On-line]. URL: http://www.votehere.net/elections.html (Accessed Sept. 5, 2001.)

[26]"Talks Break Down Between Boeing, Engineers Union," *The Wall Street Journal*, Feb. 9, 2000, [On-line]. URL: http://www.wsj.com/ (Accessed Feb. 11, 2000, but now available only to *WSJ* subscribers.)

[27]"Internet voting Technology Facilitates Rapid Resolution of SPEEA/Boeing Contract Dispute."

[28]See press release, FEC, "Commission Seeking Public Comment on Campaign Activity and the Internet," Nov. 3, 1999, [On-line]. URL: http://www.fec.gov/press/internoi.htm (Accessed May 13, 2001.)

messages, such companies may, paradoxically, be limiting the power of grassroots mobilization on the Internet.[29]

[29]Remarks by Jonal Seiger, of Mindshare Internet Campaigns at the Democracy Online Project, Public Testimony Session II, May 22, 2000, [On-line]. URL: http://democracyonline.org/taskforce/ (Accessed June 28, 2000.)

Acronyms

CBE	County Board of Elections
CEO	chief executive officer
DDOS	distributed denial-of-service (attacks)
DNS	domain name system
e-commerce	electronic commerce
e-mail	electronic mail
FEC	Federal Election Commission
FPCA	Federal Post Card Application
FVAP	Federal Voting Assistance Program
ID	identification (such as PIN)
IP	Internet Protocol
ISP	Internet service provider
LEO	local election office
NARA	National Archives and Records Administration
NASS	National Association of Secretaries of State
NRC	National Research Council
NSF	National Science Foundation
NTIA	National Telecommunications and Information Administration
NVRA	National Voter Registration Act of 1993
OSCE	Organization for Security and Co-operation in Europe
PC	personal computer
PEB	Precinct Election Board
PIN	personal identification number
R&D	research and development
SBE	State Board of Elections
SPEEA	Society of Professional Engineering Employees in Aerospace
SSL	secure socket layer (used for encryption)
UOCAVA	Uniformed and Overseas Citizens Absentee Voting Act of 1986
VIP	Voting Integrity Project
VOI	Voting Over the Internet
WWW	World Wide Web (also the Web)

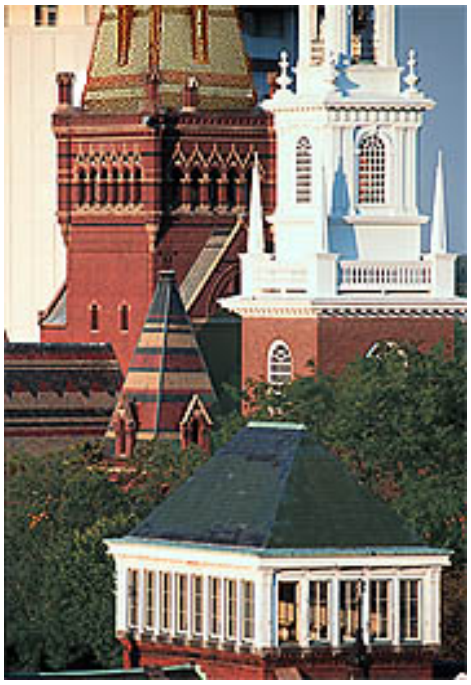
PPDDEMOCRACY

ISBN-1-879716-83-6

PIRP Home
About the Program
Program Affiliates
Latest News
Current Research
Publications
Classics
Courses and Seminars
Our People
Links to Other Sites
Finding Us

Program on Information Resources Policy

Harvard University



The Program's purpose is to help policymakers, the general public, and our Affiliates address problems brought on by changes in communications and information resources. Since 1973 we have worked with stakeholders to clarify what is at stake, how, and for whom.

Maxwell Dworkin Bldg. 125
33 Oxford Street
Cambridge, Massachusetts 02138
tel: 617 495-4114
fax: 617 495-3338
e-mail: pirp@deas.harvard.edu
URL: http://www.pirp.harvard.edu

Anthony G. Oettinger, Chairman
John C. B. LeGates, Managing Director