Democracy in Decline: Can Internet Voting Save the Electoral Process?, 22 J. Marshall J. Computer & Info. L. 409 (2004)

Bryan Mercurio

DEMOCRACY IN DECLINE: CAN INTERNET VOTING SAVE THE ELECTORAL PROCESS?

BRYAN MERCURIO†

I. INTRODUCTION

In the 2000 United States Presidential election, a lack of preparation among electoral administrators, the widespread use of outdated and inadequate voting technology, poorly developed procedural rules, and a lack of uniform standards all combined to send the once infallible American democracy into a state of emergency.[1] The world watched as Florida officials drifted from crisis to crisis in the days following the election. The world was still watching when several state and federal lawsuits failed to resolve the dilemma or determine the presidency. Finally, the Supreme Court ended the fiasco with a pragmatic, yet much criticized decision.[2] Not only did the 2000 U.S. Presidential election embarrass the nation in front of the watching world, it also served to infuriate and further alienate many Americans from the electoral process.

The majority of the problems behind the 2000 presidential debacle were caused by a long-ignored aspect of electoral governance – the method by which the people cast their ballots.[3] Effectively, this adminis-

1. For a complete review of the 2000 U.S. Presidential election, see *CNN: 2000 Election Archive*, <http://www.cnn.com/ELECTION/2000/> (accessed Jan. 15, 2003).

2. *Bush v. Gore*, 531 U.S. 98 (2000) (per curiam). For detailed discussion on the litigation and Supreme Court's decision, see Dan Lowenstein, *Lessons from the Florida Controversy*, in Realising Democracy: Electoral Law in Australia (Bryan Mercurio et al. eds. Federation Press (forthcoming) 2003); Richard Posner, *Florida 2000: A Legal and Statistical Analysis of the Election Deadlock and the Ensuing Litigation*, 2000 Sup. Ct. Rev. 1, 40-48 (2000).

3. Voting technologies have only seriously been studied in the 1950s and 1960s, when lever-arch machines became popular, and again in the 1980s, when punch cards and optical scan machines became operational. See Stephen Ansolabehere & Charles Stewart III, *Voting Technology and Uncounted Votes in the United States*, Cal Tech-MIT Voting Technology Project 1, 3 (Sept. 25, 2002) [hereinafter Cal Tech-MIT Report].

trative aspect of the electoral system has been overlooked and allowed to decline into a state of extreme disrepair without anyone taking notice. When officials were forced to take notice, two major problems emerged. First, a poorly designed ballot system served to confuse a significant portion of the voters, causing many voters to cast their ballots for an unintended candidate or unintentionally spoil their ballots. Second, a poorly designed ballot paper made it difficult to determine the intent of the voter and a poorly designed tabulating process led to electoral officials making such determinations (when possible) without a standardized system to guide their determinations. These two factors combined to wreak havoc on the electoral system and reduce the reliability and integrity of the American democracy.

Even more demoralizing to the American democracy, since the 2000 Presidential election, we have been bombarded with reports of lost, stolen, bought, and misplaced votes.[4] Similarly, reports of potential voters being turned away from the polls or otherwise disenfranchised from the electoral process have become increasingly common. The fact that in the 2002 Florida Congressional election, just two years after the presidential debacle, Broward County misplaced 103,222 votes should be highly worrying.[5] While many Americans believe that these reports only pertain to Florida, the reality is that reports of electoral misgivings are not isolated and encompass every state in the nation. In fact, the entire electoral system is in such a state of decline that an estimated 2.2 million votes have gone uncounted in each of the last four presidential elections.[6]

The American democracy depends on full and free elections, but as it stands today, voters have no real assurance that their votes are properly cast or that their votes will not get lost or uncounted for any of a number of reasons. The system by which we exercise our democratic right has repeatedly proven itself to be untrustworthy and dysfunctional. As a result, voter confidence in the system is at an all-time low. The time is now ripe to thoroughly investigate alternative methods of casting ballots as a way to restore our fledgling democracy.[7]

---

4. Whether in print or on the Internet, reports of electoral malfeasance are now common. *See* What Really Happened, *Election Fraud 2002*, <http://www.whatreallyhappened. com/votefraud.html> (accessed Sept. 29, 2003).

5. Scott Wyman, *Broward officials misplace 103,222 votes, but outcomes are unchanged*, S. Fla. Sun-Sentinel (Nov. 7, 2002).

6. Ansolabehere, *supra* n. 3, at 11.

7. In response to the 2000 electoral crisis, Congress passed the Help America Vote Act (HAVA), which authorized $2 billion in 2003 and $4 billion over three years to assist the states in improving voting technology. The 2003 Bush budget only sought $500 million for the project, but Congress reached an agreement to provide $1.5 billion in funds to implement the HAVA in 2003. Rob Ritchie, *Fair Elections Update*, <http://www.fairvote.org/ e_news/030214.htm> (Feb. 14, 2003).

Using the Internet to assist the electoral system is one possible option that is currently being considered to remedy many of the defects within the electoral process. Internet voting has the capacity to enhance the electoral process in numerous ways, such as preventing over-votes, reducing invalid votes, assisting non-English speakers with voting, allowing disabled Americans to vote without assistance, increasing participation in the electoral process, and eliminating the tons of waste generated from unused ballot papers. The endless capabilities of Internet voting do come with a caveat: Internet voting is untested and less transparent than traditional voting.

This article evaluates the ability of Internet voting to improve the electoral process by comparing it against traditional methods of voting currently used. In order to clearly understand electoral issues, Part II briefly describes the criteria needed in order to conduct a successful election. Part III introduces and defines the different forms of "Internet voting" used in the context of this article. Part IV introduces and analyzes some major faults with the election system and evaluates the promise of Internet voting as a solution to these faults. Part V reviews and substantially discredits the perceived problems with implementing Internet voting. Part VI puts forward several proposals leading to the gradual introduction of Internet voting into the electoral landscape.

II. CRITERIA FOR A SUCCESSFUL ELECTION

In order to ensure free and fair elections, any new voting measure must satisfy certain fundamental standards of elections. When reading the list of fundamental standards detailed below, it is important not only to consider whether Internet voting (or any new election system) meets a substantial portion of the criteria, but also how the new system relates and interacts with other aspects of democracy such as access by demographic groups, election logistics and administration, deliberative and representative democracy, and the political culture of elections.[8] The criteria for a successful election are set out below:
—Authentication and Eligibility – only authorized and eligible voters should be allowed to cast ballots;
—Accuracy –votes should be recorded and counted correctly, to ensure that the will of the people is represented;
—Uniqueness – voters should only be allowed to cast one ballot each;
—Integrity – votes which are forged, modified or deleted should be detected;

---

8. For instance, a move to increase security in the voting process would increase the costs of running an election and reduce voter convenience and flexibility. Likewise, a move to encourage participation could lead to a reduction in authentication and verifiability.

—Verifiability and Auditability – verification that all the votes have been accounted for in the final tally and that reliable and authentic records exist to that effect;

—Reliability – election systems should ensure against the loss of any votes, even when faced with electoral failures;

—Secrecy and Non-Coercibility – voting is done in secret without voters ever having to reveal how they cast their respective ballots;

—Flexibility – election equipment should allow for a variety of platforms and technologies and should be accessible to all voters, including those with disabilities;

—Convenience – voters should be able to quickly cast their ballot without undue delay;

—Certifiability – election systems should be regularly tested and certified to ensure against electoral failure;

—Transparency – voters should possess a general understanding of the voting process and should not be deceived into voting a certain way; and

—Cost-effectiveness – election systems should be affordable while still being efficient and effective.[9]

III. WHAT IS INTERNET VOTING?

The term "Internet voting," or "online voting," is not clearly defined. "Internet voting" is an online form of "electronic voting" (e-voting). The term "Internet voting" has became synonymous with remote Internet voting when in fact it could mean any form of voting on the Internet, whether at home, the polling station, voting kiosk, or any other place in which the Internet is accessible. As the benefits and burdens of Internet voting depend upon which version of Internet voting is on offer, this article will differentiate between and clarify which form of Internet voting is being discussed.

Confusion also exists within the term "electronic voting." While the term can be used broadly to describe any form of mechanical voting, such as punch card machines or voting at the polling station using a computer terminal or any similar touch-screen or mouse activated machine which stores votes and may or may not have the ability to tabulate votes, these forms of e-voting are not online forms of voting, meaning the systems are

---

9. This criterion was compiled from a White House commissioned report operated by the U.S. National Science Foundation, Internet Policy Institute and the University of Maryland. The report was the product of an October 2000 workshop, where political scientists, computer scientists, election officials, and others analysed and assessed the feasibility of Internet voting and identified research priorities for the advancement of Internet voting. Internet Policy Institute, *Report of the National Workshop on Internet Voting: Issues and Research Agenda* 11, <http://e-voto.di.fc.ul.pt/docs/InternetVotingReport%20-%20March%202001.pdf> (2001) [hereinafter IPI Report].

not connected to Internet lines and there is no chance of outside interference (e.g. hackers). This article will not discuss offline e-voting, instead this article focuses on Internet-based, online voting.

With this background in mind, electoral commissions considering implementing online e-voting have two very distinct forms to consider.

A. REMOTE INTERNET VOTING

Modern life has wholeheartedly embraced the accessibility, relative low cost, and seemingly endless capabilities of the Internet. Home computer ownership and Internet use have risen exponentially in recent years,[10] and more than 160 million Americans now do a variety of time-consuming tasks, such as banking, shopping for clothes or groceries, or paying bills online in a matter of seconds.[11] Moreover, federal, state, and local governments now rely on the Internet to provide constituents with essential governmental information and interactive services.

Despite the inclination to treat our electoral democracy with judicious care, voters are calling for more convenience to the voting process.[12] Remote Internet voting would provide the extra convenience, as it would allow voters the opportunity to cast their ballots in the comfort of their own homes, at an Internet café, or anywhere else the Internet is accessible. Proponents of remote Internet voting envision voters logging onto the voting Web site via secure means, establishing their identity, and then voting in a real-time transaction at any time convenient to the voter on Election Day. This formula is simple to understand and similar to any other web-based transaction. However, remote Internet voting will be the most difficult form of e-voting to implement, as cost, security, and policy-related issues must be adequately addressed before its full-scale implementation.[13]

---

10. The World Wide Web expanded from 50 servers in 1993 to over 100,000 in 1997. *See* Ari Staiman, *Shielding Internet Users from Undesirable Content: The Advantages of a PICS based Rating System*, 20 Fordham Intl. L.J. 866, 874 (1997). As of March 2003, the Internet had over 649 million users. Global Reach, *Global Internet Statistics*, <http://www.glreach.com/globstats> (accessed June 20, 2003).

11. *See* Global Reach, *Details of country/language analysis*, <http://global-reach.biz/globstats/details.html> (accessed June 20, 2003).

12. A recent study revealed sixty-one percent of younger voters are "enthusiastic" about voting online. *See Six Out of Ten Young Voters Say Yes to Internet Voting*, Business Wire (July 23, 1999); *Voters Overwhelmingly Support Internet Voting*, Business Wire (Mar. 1, 2000) (reporting a poll conducted by Votehere.com indicated ninety-four percent of the 3,638 polled indicated a desire to have Internet voting offered as a voting option in the future).

13. Remote Internet voting depends on a number of factors outside the electoral officers' control, such as whether the voter's operating system is supported by the proper voting and encryption software and whether the voting system is able to recognise that the person attempting to vote is a legitimate voter who has not previously voted in the election.

Several binding and non-binding elections have trialed remote Internet voting recently, with the 2000 Arizona Democratic Primary garnering the most considerable media attention. In that election, voters could voluntarily choose to cast their ballots online or by traditional means. The trial, trumpeted as "the first-ever, legally-binding public election over the Internet," succeeded in increasing voter interest and suffered no breach of security or electoral failure.[14] This landmark trial should be commended for putting Internet voting on the agenda and for starting the Internet voting revolution.

The U.S. Department of Defense Federal Voting Assistance Program also developed and trialed an Internet voting system for military personnel located outside the U.S.[15] While the trial took some years to develop and the cost incurred proved considerable,[16] the end result was a successful trial at the 2000 Presidential election.[17] The government has already announced that it will expand this trial in the 2004 general election and provide Internet registration and voting for overseas citizens as well as military personnel.[18]

The Alaska Republican Party also conducted a straw poll over the Internet in 2000. Alaska is a sparsely populated state where travel in the winter is severely limited, making it difficult for a number of potential voters to get to a polling station to cast their ballots. Such a situation almost certainly dissuades people from voting and lowers the overall participation rate of Alaska. The Republican Party recognized this problem and decided to trial Internet voting as a possible way of increasing voter participation. The trial, conducted without the support of the

---

14. John O'Looney, *The Implications of Internet Voting*, <http://www.govtech.net/maga zine/gt/2000/sept/Internet/implications/phtml> (accessed May 19, 2002).

15. Voters were covered by the *Uniformed and Overseas Citizens Absentee Voting Act* (42 U.S.C. § 1973). Eligible voters must have had legal residence in one of the counties allowed to participate in the trial (each State was limited to only one county participating in the trial measure to limit risk exposure in the event of system failure).

16. The trial proved costly for a number of reasons. First, the Defense Department funded the complete development of the e-voting system. Second, the Defense Department had to organize and train participants and state and local election officials for the trial. In this regard, support from individual states was crucial, as each of the four states involved amended its legislation to allow the 250 trial lists to cast their ballot over the Internet. Third, the Defense Department provided each voter with an individualized PIN and CD-ROM to guarantee that each web browser being used by the voter had adequate security and technical compatibility capabilities.

17. The Federal Voting Assistance Program (the agency which administered the trial) report evaluating the trial is available at <http://www.fvap.gov/voi.html>.

18. The Federal Voting Assistance Program is developing a system called the "Secure Electronic Registration and Voting Experiment" to implement these measures for the 2004 elections. At present, fourteen states are participating in the project. *See* Digital Government Program, *Military Voting Goes Online*, <http://www.diggov.org/news/stories/2002/0402/0402military_holland.jsp> (accessed Jan. 15, 2003).

Alaska Division of Elections, proceeded without delay or any security problems.[19]

Internet trials are also occurring outside the U.S., with European countries, such as Switzerland[20] and the United Kingdom (UK),[21] having trialed remote Internet voting in binding elections and Estonia already having successfully implemented remote Internet voting.[22] Several other countries around the world are also studying Internet voting due to its efficiency, speed, and ability to increase voter participation.[23]

---

19. The Republican straw poll allowed voters in three territories to cast their ballots over the Internet either remotely or at the polling station. Sam Diaz, *Arizona Democrats Can Vote Online in Primary*, Knight-Ridder Trib. Bus. News (Mar. 3, 2000).

20. In order to combat falling turnout, the Swiss canton of Geneva recently staged its first Internet election. Voters praised the system for its efficiency and accuracy. Alison Langley, *Geneva Suburb Casts Ballots on the Internet in Test Project*, N.Y. Times (Jan. 12, 2002).

21. In May 2002, the British government provided £3.5 to undertake a series of initiatives aimed at improving electoral efficiency, encouraging voter participation and widening the range of voting methods. The trials allowed electorates to conduct voting via the Internet, text messaging or offline e-voting at the polling station in thirty local electoral districts. *See* Electoral Commission, *Modernising Elections*, <http://www.electoralcommission.gov.uk/about-us/modernisingelections.cfm> (accessed Jan. 9, 2003); *Britain Experiments With Early, High-tech Voting*, AP World Politics (April 25, 2002). Prior fears of security breaches and increased electoral fraud appeared unfounded, as the system functioned properly and there were no technical glitches or security breaches. In addition, e-voting improved the accuracy and efficiency in the ballot tabulation process and voters rated the system highly. The primary aim of the trial, to establish the reliability and security of the e-voting systems and to build public confidence in the new technologies, achieved its objectives. *See Online Voting Fraud Warning*, <http://www.news.bbc.co.uk/hi/English/uk_politics/newsid_1799000/1799883.stm> (accessed June 9, 2002); Wendy Brewer, *E-voting Has a Long Way to Go: Election Results Mixed for Alternative Voting Methods*, PC Advisor (May 3, 2002). In May 2003, the UK expanded the trials by allowing over 1.5 eligible voters in forty-two electorates the opportunity to vote using the new voting methods. The trial, costing £18 million, chiefly aimed to improve voter participation and enable the UK to have an online general election by 2006. *See* Matthew Tempest and Martin Nicholls, *E-Vote Early, E-Vote Often*, The Guardian (April 17, 2003).

22. Dermot McGrath, *Europeans Eye E-Vote Eventuality*, Wired News (Apr. 22, 2002); *See* Matthew Tempest, *Reformers Skeptical of Online Voting*, The Guardian (Jan. 7, 2002).

23. Several European countries, including Sweden, Ireland, Holland, and Norway are studying Internet voting with a view to implementing it in future elections. In addition, Germany announced it will have online voting by 2006 and France, Italy, and Spain have planned e-voting trials in forthcoming referenda and elections. Eileen McGann, *Is Internet Voting Fair?*, Network World 61 (June 26, 2000). A number of these initiatives were funded by the European Union. Cybervote Project, *Vote in Total Confidence Via the Internet*, <http://www.eucybervote.org/press_release.html> (Oct. 13, 2000).

B.   INTERNET VOTING AT THE POLLING STATION

While the long-term promise of remote Internet voting is great, many view another Internet-based option, Internet voting at the polling station, as the more viable short-term option. Internet voting at the polling station is similar to the processes voters know and trust. The voter would appear at the polling station on the requested day and have his or her name marked off the role as normal before retiring to a booth which, instead of being equipped with traditional voting apparatus, would have a terminal connected to a closed network server at which the voter could cast a ballot electronically. The computer would then forward the votes via modem to a central location for counting and collating.[24]

Internet voting at the polling station is practical and appealing, as it offers greater convenience and efficiency over traditional voting while also allowing election officials to maintain control over the computer operating system as well as monitor the physical surroundings of the venue, making the security risks more manageable and the risk of electoral failure significantly less than with remote Internet voting. This control would also provide as much guarantee to authentication and privacy as traditional paper voting and, as the voting software would not allow multiple votes, eliminate the possibility of anyone voting more than once under the same name.

While voters would not have the convenience of voting away from the polling station, they would get numerous benefits from Internet voting at the polling station, such as fast and simple voting as well as quicker, more accurate election results. Election officials would also benefit from Internet voting at the polling station from the added efficiency and diminished administrative burden. Officials could also use Internet voting at the polling station as an evolutionary system towards remote Internet voting.

Internet voting at the polling station has been successfully trialed in non-binding elections by numerous software companies. The most notable private software companies include VoteHere.net,[25] Election.com,[26]

---

24. The vote forwarding process would occur either during the election or after polling closes. For instance, the system could "store and forward" the voting data by secure means to the central server during the election to prevent flooding and data loss if the communication lines fail. Conversely, the computer could record and store votes in a localised server at each polling station before sending the final count via secure connection to a central server.

25. VoteHere.net conducted a trial in the State of Washington at the 1996 Presidential election. The trial aimed to introduce the concept of e-voting to the electorate. After voting in the binding election, voters could elect to cast their non-binding vote at an Internet voting stations. The e-voting system was well received by the majority of those who participated. VoteHere.net also performed the Alaska straw poll and has tested its technology at polling stations in Washington, Iowa, Illinois, and Virginia, with very favorable responses from voters who have tried the system. Margaret Johnston, *Remote Alaskans to Vote Using*

and Safevote.com.

In November 2000, Safevote.com conducted one of the most comprehensive mock elections in Contra Costa County, California. Safevote.com invited voters who cast their pre-poll vote to cast a mock vote via the Internet at the same location. Voters participating in the trial were given a PIN[27] and once the system was activated, used a mouse to select their preferred candidates. Once voting was completed, the votes were stored on a completely separate system to prevent the voter's identity from being traced from his or her vote.[28]

In addition, Safevote.com encouraged people to hack into the system and even published the hardware and software details on the Internet, hosted an attack help page, and created an attack hotline to encourage hackers to attempt to crack the security code. The system remained secure throughout voting. Safevote.com attributes their record of security to the use of a constantly changing IP address used to connect the system to the Internet, which made flooding the system and hacking difficult, if not impossible.

Recently, several companies have started conducting shareholder votes via the Internet on a wide range of topics, and several private companies have been given an opportunity to showcase their voting software.[29] While public elections attract more publicity and passion and have to comply with more rigorous standards, private elections conducted over the Internet contribute to the development of better voting software by allowing companies to assess and correct performance after each vote and are a useful platform for election officials to trial Internet voting software.

Internet, Network World Fusion (Jan. 24, 2000). Votehere.com also conducted the recent UK trials, and it has agreed to provide Internet voting facilities to Sweden, Finland, Germany and other European countries. *See VoteHere Partners With Votia to Offer Online Voting in Sweden and Other European Countries*, <http://www.votehere.com/news.htm> (Jan. 9, 2002).

26. Election.com managed the election for the Arizona Democrats, the board of directors of ICANN (Internet Cooperation for Signed Names and Numbers), the Australian NRMA Board of Directors and many other elections. Election.com, *Press Releases*, <http://www.election.com/us/pressroom/pressrel.htm> (accessed June 24, 2003).

27. The PIN numbers were calculated using voter's date of birth and the type of ballot requested. The voter verification system checked the PIN against the database and enabled the voter to verify their vote before submitting it for tally.

28. This security and privacy measure is common among all the major e-voting software companies.

29. Derek Dictson & Dan Ray, *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*, White Paper, <http://www.securepaper.votingpaper.com> (Jan. 2002).

IV. WHY ADOPT INTERNET VOTING

Recent elections have underscored the failure of the current system to protect critical elements of an electoral process. The current system has proven ineffective at preventing or detecting forged, modified, or deleted votes, and loses, misplaces or otherwise leaves millions of votes uncounted in each presidential election. Moreover, millions more Americans are prevented from voting for any number of reasons, including faulty prison records or improperly mailed registration cards. These problems signal a major systemic failing of our electoral system and have correctly led many Americans to question the reliability and accuracy of the current voting system.

This section introduces and analyses some major faults with the current election system and evaluates the promise of Internet voting as a solution to these faults. The section is divided into four distinct sub-sections, each offering another failing of the current system and argument in favor of Internet voting as a more accurate and reliable method of voting.

A. LOW PARTICIPATION RATE

In 2000, just over half of the eligible voters in the U.S. actually cast a ballot in the presidential election. In an election literally decided by a few hundred votes, this statistic rightly casts doubt upon the democratic nature of the government.

More worrying is the fact that the 2000 election statistics are not an aberration. In fact, the 2000 election followed the four-decade old trend of declining voter participation.[30] The declining rate of participation has finally emerged as the paramount concern among both academics and policymakers and several recent studies have concluded that the problem of falling voter participation may warrant the implementation of Internet voting.[31]

Advocates of Internet voting feel the technology removes the two main obstacles to voting – convenience and mobility[32] – and will particu-

---

30. Wired News, *Report Pans Internet Voting* ¶ 10, <http://www.wired.com/news/print/ 0,1294,42229,00.html> (March 6, 2001). The need to increase participation in the electoral process is evidenced by the fact that ten million fewer Americans voted in 1996 than in 1992, resulting in participation that was its lowest since 1920 when the 19th Amendment gave women the right to vote.

31. IPI report, *supra* n. 9, at 24; California Secretary of State, *California Task Force on Internet Voting* 36, <http://www.ss.ca.gov/executive/ivote/> (accessed May 7, 2002) [hereinafter *California Task Force on Internet Voting*].

32. The U.S. Census bureau concluded voter apathy and a lack of voter convenience were the main reasons behind the low turnout. A recent study also places some of the blame for low participation on poor accessibility of polling stations (long commutes and inconvenient locations), which must adhere to the stringent requirements of the ADA. *See*

larly increase participation among the traditionally under-represented groups, such as younger voters, elderly voters, and disabled voters.[33] Remote Internet voting would also particularly suit voters called out of town at the last minute, who instead of being disenfranchised, would be able to exercise their civic duty.

The U.S. is not the only country experimenting with Internet voting as a potential solution to voter apathy, as the UK is also currently studying and trialing the technology with a view towards increasing voter participation.[34] Both the U.S. and UK have also instituted other reforms to increase participation, such as simpler registration procedures, liberalizing the absentee ballot requirements, and extending voting times, but these reforms have had little or no effect on voter participation.[35] As a result, both nations have indicated a willingness to substantially invest in and trial Internet voting as a possible cure to the modern day lethargy, and leading British parliamentarian Sir Robin Cook believes implementing Internet voting at the next general election is a way to "enfranchise" disillusioned voters back to the democratic process.[36]

Internet voting has successfully generated election-time interest and attracted voters to the polls.[37] For example, despite the fact that Vice

James G. Gimpel & Jason E. Schuknecht, *Political participation and the Accessibility of the Ballot Box*, <http://www.vote.caltech.edu/Links/gimpel1.pdf> (forthcoming in Political Geography, 2003). The study found turnout is heaviest in densely populated areas and lightest in suburban areas (due to long commutes, busy schedules and inconvenience polling places). *Id.*

33. A Federal Elections Commission report shows that people aged 18-24 are the least likely to vote. In 1996, less than one-third of 18-24 year olds voted in the presidential election. Federal Elections Commission, *Voter Registration and Turnout in Federal Elections by Age 1972-1996* <http://www.fec.gov/pages/agedemog.htm>. The Public Policy Institute of California reports that 73 percent of 18-24 year old Californians either often or sometimes have access to the Internet and e-mail, making it likely that participation will rise under Internet voting. *California Task Force on Internet Voting, supra* n. 31, at 43.

34. Britain managed only a fifty-nine percent turnout for the last general election, thought to be at its lowest point since universal suffrage was introduced. Jackie Ashley, *Sir Robin Cook, Leader of the House of Commons, Plans to Make UK First to Vote on Internet*, The Guardian (Jan. 7 2002).

35. While these measures serve to reduce the level of security and integrity of the election, they have failed at attracting the disenchanted voter to the polls. *See* e.g., a January 28, 2003, election in Orange County, California, where 24,258 of the 35,646 ballots cast (sixty-eight percent) were from absentee voters (the highest rate of absentee voters ever in a California election); unfortunately, only 12.9 percent of the 277,007 registered voters participated in the election. Orange County, *Orange County Registrar of Voters*, <http://www. oc.ca.gov/election> (accessed Mar. 10, 2003).

36. Ashley, *supra* n. 34.

37. On the other hand, some commentators suggest Internet voting may only be a short-term solution to voter apathy and that its implementation could be perceived as undermining civic participation and the legitimacy of the act of voting, actually depressing long-term participation. IPI, *supra* n. 9, at 25.

President Al Gore had already secured his party's nomination, the 2000 Arizona Democratic primary, which allowed voters to cast their ballots over the Internet, saw voter participation rise 600 percent over the prior election, with forty-one percent of the 86,907 votes cast via the Internet. Internet voting also appears to have assisted the Reform Party in increasing their 2000 Presidential candidate nomination total.[38] In addition, Internet voting is also credited with raising voter participation from fifty percent to sixty-four percent in the recent legally binding referendum in Switzerland.[39]

In addition, computerized voting has proved popular with mainstream voters, with statistics showing voters who have used both remote and polling station Internet voting systems in the U.S. and UK overwhelmingly rate the process very highly and uniformly praise on the ease of use, speed, and assistance provided by the system.[40] Computerized voting has also been praised by non-traditional voters, such as non-English speakers and disabled voters.[41] This praise stems from the fact that computerized voting's flexible format can accommodate more voters than traditional voting methods. For example, while traditional voting is limited to the amount of voters it can accommodate (due to issues such as printing costs), computerized voting can accommodate as many different languages as required without adding significant cost to the system. Moreover, computerized voting is also well received by disabled voters worldwide, including blind voters, who are often unable to cast a ballot without assistance from electoral officials under traditional voting.

---

38. Farhad Manjoo, *Wired News, Reform Voting Evokes E-Votes*, <www.wired.com/news/politics/0,1283,37964,00.html> (accessed Aug. 3, 2000).

39. SiliconValley.com, *Swiss Village Holds First Internet Vote*, <http://www.silicon valley.com/mld/siliconvalley/news/4985064.htm> (Jan. 24, 2003).

40. *See* Farhad Manjoo, *The Case for Electronic Voting*, <http://www.wired.com/news/politics/0,1283,40141,00.html> (accessed Nov. 14, 2000) (reporting Riverside, California's offline e-voting recently received a ninety-nine percent user-approval rating); NOP Research, *Public Opinion in the Pilots*, <http://www.electoralcommission.org.uk/templates/search/document.cfm/6267> (accessed Oct. 21, 2002) (reporting forty-five percent of those polled thought that e-voting made the process of voting "better"); ACT Electoral Commission, *Electronic Voting Trial 'A Success,'* <http://www.elections.act.gov.au/adobe/2001Elec tionReviewComputerVoting.pdf> (accessed June 28, 2002) (reporting eighty-nine percent of voters found e-voting easy to use and understand). In addition, in a non-binding trial operated by Safevote.com, 100 percent of the 300 people who voted using the system found it easy to use and understand, including an eighty year old woman who had never used a computer and a drunken man, who stated, "If I can do this, anyone can." Farhad Manjoo, *Ballots Need an Upgrade – Duh!*, <http://www.wired.com/news/politics/0,1283,40078,00. html> (accessed Nov. 10, 2000).

41. Thad Hall, *LA Story: The 2001 Election*, <www.reformelection.org/data/reports/la-hall.pdf> (accessed Jan. 5, 2003) (reporting countless non-English speaking Americans in Los Angeles required assistance to vote with a paper ballot).

B.　EQUALITY ISSUES

While critics claim that the implementation of Internet voting may violate equality laws, deny or unfairly disadvantage some groups in the community the right to equality and equal access, further dilute the minority vote, and increase the "digital divide," this section will show not only that Internet voting meets the equal rights standards but also that the *current* system of voting violates the equality requirements and denies some groups in the community the right to vote and that Internet voting will allow *more* people to vote and grant the equal franchise to many communities that are without equal representation under the current system. The section will further show that leaving the current voting system unchanged will only increase the "voting technology divide" and promote the unfair treatment of disabled and minority voters.[42]

1.　*Minority Voting Under the Present System*

The statistics from the 2000 Presidential election are clear: minority votes are more likely to be miscounted, misplaced, disregarded, or otherwise uncounted than that of Caucasian voters. This inequality is primarily due to the fact that minority precincts cannot afford to purchase state-of-the-art voting machines and are forced to rely on outdated voting technology to record and count the vote.[43] For example, the Florida county of Gasden, the only Florida county where black voters make up a majority of the electorate, is a poor county that uses outdated voting technology. As a result, in the 2000 election, voters in Gasden had a sixty-eight times greater chance of having their votes deemed invalid than in adjoining Leon County, a county that could afford to purchase the latest voting technology.[44]

This scenario of one county using unreliable voting technology while another county in the same state uses a more reliable method of recording and tabulating votes creates a "voting technology divide." In the 2000 election, over 2000 Gasden County votes were deemed invalid in an election decided by only 537 votes, leading one to question whether differences in voting technology have the potential to alter state-wide election outcomes.[45] As only nine states voted with uniform or near-uniform technology, this gap is not peculiar to Florida. Instead, the "voting technology divide" is present in almost every state in the nation.

---

42. To the author's knowledge, the term "voting technology divide" first appears in Paul Schwartz, *Voting Technology and Democracy*, 77 N.Y.U.L. Rev. 625 (2002).

43. *A Modern Democracy That Can't Count Voters*, L.A. Times A1 (Dec. 11, 2000). As each county has to fund the cost of voting equipment, the poorer counties cannot afford $5,000 on proper technology. Schwartz, *supra* note 42, at 3-644.

44. *Id.* at 625-26.

45. *Id.*

Many post-2000 investigations reveal problems with uncounted ballots are particularly concentrated in disadvantaged communities. For example, it has been found that in "many black precincts in Chicago, one of every six ballots in the presidential election was thrown out" but that the uncounted rate for suburban precincts was virtually nil.[46] Moreover, as many as one in three votes were uncounted in black sections of Jacksonville, Florida, a rate 400 percent above the uncounted rate in predominantly white precincts.[47] Black voters in Ohio also appear to have been disadvantaged, with a vast majority of the uncounted votes in that state being from poorer, predominantly black precincts.[48] These are but a few examples that prove the "voting technology divide" is real and significantly disadvantaging minority voters.

Perhaps the most convincing proof of the "voting technology divide" is the results of a study conducted by Rep. Henry A. Waxman, the ranking member of the Committee on Government Reform. The study, commissioned to examine whether voting technology can reduce the rate of uncounted ballots, even more clearly illustrates the existence and harm of the "voting technology divide."[49] Detroit was chosen as the case study location for a number of reasons, including the fact that it recently made a substantial effort to reduce uncounted ballots and the fact that it has one of the highest minority populations (African-Americans make up seventy-six percent of the population) and the highest poverty rate of any U.S. city (thirty-two percent of the population live below the poverty line).[50]

Detroit upgraded its electoral system in 1998 and replaced punchcard voting with an optical scan system that allowed voters to view and amend their ballots before leaving the polling booth. The change resulted in the overall percentage of uncounted votes in Detroit decreasing from 3.1 percent of the ballots cast in 1996 to 1.1 percent of ballots cast in 2000 (in other words, from over fifty percent above the national average in the 1996 election to almost fifty percent below the national average in 2000).[51] The city saw an across the board reduction in the number of uncounted ballots, with every precinct reducing its percentage of un-

---

46. John Mintz & Dan Keating, *A Racial Gap In Voided Votes; Precinct Analysis Finds Stark Inequity in Polling Problems*, Wash. Post (Dec. 3, 2000).

47. John Mintz & Dan Keating, *Florida Ballot Spoilage Likelier for Blacks; Voting Machines, Confusion Cited*, Wash. Post (Dec. 3, 2000).

48. Darrel Rowland, *Many Votes Uncounted in Ohio's Poor Areas*, Columbus Dispatch (Dec. 17, 2000).

49. *Election Reform in Detroit: New Voting Technology and Increased Voter Education Significantly Reduced Uncounted Ballots*, Minority Staff Special Investigations Division, Committee on Government Reform, U.S. House of Representatives. Prepared for Rep. Henry A. Waxman, Ranking Member (Apr. 5, 2001).

50. *Id.* at 4.

51. *Id.* at 1.

counted votes from 1996 to the 2000 election and some precincts reducing their uncounted rate from over seven percent in 1996 to less than one percent in 2000.[52]

Another study, conducted by the Cal Tech-MIT Voting Technology Project, also revealed the true effects of the "voting technology divide." The study found that voting equipment has strong and "substantial effects" on the rate of uncounted votes, with the difference between the best performing voting equipment and the worst performing voting equipment being as much as two percent of ballots cast. As five of the last twenty presidential elections have been determined by less than two percent of the vote, this finding casts doubt on the reliability of many past election results.[53]

Both studies confirm the existence of a "voting technology divide" and the direct correlation between voting equipment and the rate of invalid votes. These studies provide clear evidence that if we ignore this problem and keep the current system of voting, minority vote dilution and other equality problems will only increase.

2. *Minority Voting and the Internet*

The "digital divide" has emerged as the primary federal constitutional issue regarding Internet voting. In electoral terms, the fear is that giving voters another means of voting will increase voter participation among one group (people who have Internet access) while voting participation rate remains static in other voting groups (non-Internet users). While increasing voter participation is one very persuasive reason for adopting Internet voting, the concern is that this "digital divide" will result in greater voter participation among educated and wealthier voters at the expense of less educated and poorer voters.

Proponents of this argument claim that the implementation of Internet voting would violate the 15th Amendment's guarantee that "the right to vote shall not be denied or abridged by the United States or by any state on account of race or color."[54] They base this argument on the assumption that minority voters do not have as much Internet access as Caucasian voters.[55] While the constitutional argument is tenuous under

---

52. *Id.*

53. Ansolabehere, *supra* n. 3, at 28.

54. U.S. Const. amend. XV, § 1.

55. An additional argument could be made under the *Voting Rights Act* of 1965, which states in pertinent part: "To assure that the right of citizens of the United States to vote is not denied or abridged on account of race or color, no citizen shall be denied the right to vote. . . because of his failure to comply with any test or device in any State. . . ." 42 U.S.C. § 1973(b). Internet voting could possibly violate the Act by broadening the access of voting to one segment of the population who has access to a "device" that is unavailable to other segments of the population. As Internet voting produces a far lower rate of invalid votes

any circumstances, the statistics regarding Internet use do not necessarily substantiate the claim that minorities use the Internet substantially less than white voters.

A National Telecommunications & Information Administration (NTIA) study shows that the perceived digital divide between white and minority voters, educated and uneducated voters, and wealthy and poor voters to largely be misstated. The study revealed that Internet access among Caucasians (29.8 percent), black-Americans (25.5 percent), and Asian/Pacific Islanders (thirty-six) are relatively equal. The study found that two groups Native Americans (nineteen percent) and Hispanics (12.6 percent) clearly lag behind the other groups.[56] It also appears that the so-called digital divide among those highly educated and those without an education is also illusory, as 53.1 percent of those with only a high school education regularly use the Internet. Moreover, income level also appears not to be a determining factor, with forty-one percent of adults with an income under $15,000 and sixty percent of adults with incomes of $15,000-$49,000 using the Internet.[57]

In addition, the government has devoted large amounts of resources to programs aimed at narrowing the "digital divide" and all indications are that the programs appear to be working, with minority participation on the Internet rapidly growing.[58] Furthermore, during the 2000 Arizona Democrats Internet trial, Internet voting not only succeeded in a record setting total turnout, but the feared effect of the digital divide proved illusory. In fact, Native American turnout was four times that in previous elections, despite the fact that only nineteen percent of Native Americans have regular Internet access.[59]

---

when compared to traditional forms of voting, people without access to Internet voting would be deprived of equality in the voting process. If it can be shown that a certain segment of the population is disadvantaged by this disparity, then the system of Internet voting could be challenged as offending policies of equality and equal access. Regardless of the rate of invalid votes, remote Internet voting could add an extra incentive encouraging those groups with Internet access to vote, which could be seen as a fundamental inequality, as voting results would be affected by the change in voting patterns of one voting demographic. While this argument, and the argument in the preceding paragraph, would carry weight in a system relying totally on remote Internet voting, election officials should avoid fundamental inequities by having remote Internet voting as an alternative to, and not a replacement of, polling station voting.

56. Jerry Kang, *Cyber-Race*, 113 Harv. L. Rev. 1131, 1163 (2000).

57. William E. Kennard, *New Approaches to Minority Media Ownership: Columbia Institute for Tele-Information, Columbia University: Foreword: Equality in the Information Age*, 51 Fed. Comm. L.J. 553, 554 (1999).

58. *Id.* at 555.

59. Andre M. Chernay, University of the Pacific, McGeorge School of Law, *Analysis of Internet Voting Proposals*, <http://www.mcgeorge.edu/government_law_and_policy/califor nia_initiative_review/reports/ccglp_cir_reports_internet_voting.htm> (accessed June 30. 2003). Seventy-eight percent of the Native American community in Apache County partici-

Surprisingly, the Arizona Internet election was almost halted before it began due to a lawsuit filed by the Voting Integrity Project (VIP). The VIP argued the election denied equal access and discriminated against certain voters because Internet voting would last four days instead of the usual one day period, but the judge questioned the digital divide data and stated the availability of county owned computers with Internet access for voters' use were enough to deny the injunction.[60] The Justice Department supported the ruling and stated that Arizona's proposed implementation of Internet voting had no inherent conflicts with minority groups.[61]

The Constitutional issues regarding equality standards do not seem insurmountable. The Department of Justice has stated that the constitutional arguments are not valid so long as sufficient Internet access is provided to the public.[62] Therefore, as long as polling booths remain open to accept voters, Internet voting should not be viewed as disadvantaging a particular voting group. Moreover, when compared with the inequality stemming from the current system, a system which required the use of third-world election monitors in the 2002 election to stem the uncertainty lingering from the 2000 election, the potential problems of Internet voting seem minor.[63]

3. Disadvantaged Voters and the Internet

Another equality-based argument often used against Internet voting is that some voters will not be able to keep up with or understand the technological advancement. While it is true that every potential voter could not vote electronically, the traditional methods of voting currently exclude many Americans from voting without assistance. Internet voting would finally allow those voters the right to cast their own ballots.

Under the current system, a large portion of disabled voters, including blind voters and those with limited arm movements, are denied the right to vote in secret due to the limited number of voting methods offered. A properly designed e-voting machine at the polling station would

---

pated in the election, as did 53.1 percent of the Native American community in Navajo County. *Id.*

60. *VIP v. Fleisher*, No. CIV 000109 Phx. Pgr (D. Ariz. Jan. 21, 2000).

61. Chernay, *supra* note 59. Interestingly, VIP's argument contradicts their position in a paper entitled, "Are We Ready for Internet Voting," which argues voter convenience would lower participation among Internet users, thereby serving not to decrease minority voting power but actually increasing the power. *See* O'Looney, *supra* n. 14.

62. Brian Krebs, *Net Voting Standards Proposed*, <http://www.computeruser.com/newstoday/00/02/29/news8.html> (Feb. 29, 2000).

63. *Group to Monitor Fla. Election*, NY Times (Oct. 15, 2002) (stating that at the behest of the black community, Miami-Dade hired monitors used in developing democracies to ensure a proper vote in the 2002 elections).

finally grant those voters the opportunity to cast their ballots in secret. Trials of various forms of online and offline e-voting systems in numerous countries, including the U.S., Australia, UK, and Japan, have been universally praised for their ease of use and guidance.[64]

Without action on the part of the legislature and electoral administrators, the threat of legal action on behalf of disabled voters is a real and present possibility. While some American states already enable disabled voters the opportunity to vote in secret without assistance, a number of states continue to deny this right to its disabled citizens. In doing so, these states are risking the cost and embarrassment of a lawsuit, as the fact that some disabled voters are unable to vote without assistance, and thereby denied their right to vote in secret, even though technology exists to allow those voters to vote in secret, may violate federal or state anti-discrimination statutes.

The issue was first litigated in the District of Columbia (DC) under the *Americans with Disabilities Act 1990* (U.S.) (*ADA*).[65] The case settled before trial, however, so no authoritative ruling on the issue was made. But the settlement signified a complete victory for the plaintiffs, with the electoral commission agreeing to purchase and make available a number of disabled-accessible e-voting machines at each polling station.[66] Since that litigation, other states having voting methods inaccessible to blind or visually impaired voters have come under attack from disabled groups such as the American Association of People with Disabilities (AAPD) and other groups, including the American Civil Liberties Union (ACLU). While several states have acted on their own accord and provided funding for the purchase of accessible voting equipment, other states have

---

64. *But see e.g.* Colin Barry, et al, *Electronic Voting and Electronic Counting of Votes: A Status Report*, at 12, 14, <http://www.eca.gov.au/reports/electronic_voting.pdf> (accessed May 15, 2002) [hereinafter *Status Report*]; IPI Report, *supra* n. 9, at 25 (advancing the proposition that poll site e-voting allows more people with disabilities access to voting than any other voting method). Ardis Bazyn of the California Council of the Blind stated "We give touch screen voting machines an "A" for giving blind and visually impaired voters an independent and private way to vote. With electronic voting, we have the ability to hear our vote choices read through a headset, and cast a vote and confirm using a keypad. Voters can also enlarge the print on the screen to vote." California Voter Empowerment Circle, Press Release, July 2003 (on file with author).

65. The U.S. has an estimated 54 million disabled citizens, with 24 million of voting age. *Disabled U.S. Voters Have Their Say*, <http://www.accessibility.com.au/news/internat/us_voters.htm> (accessed Mar. 11, 2003).

66. American Association of People with Disabilities, *AAPD Plaintiff in a Landmark Lawsuit Against the District of Columbia That Has Just Been Settled*, <http://www.aapd.com/dvpmain/votemachines/landmarksettledcvotemach.html> (accessed Jan. 5, 2003) [hereinafter *AAPD Plaintiff*]; Perry Bacon, *Optical-Scan Ballot Debuts for Primary; Write-In Count Will Not Benefit*, Washington Post T03 (Sept. 5, 2002).

fought the issue all the way to the courthouse.[67]

For instance, one blind voter in Maryland filed a compliant after election officials refused to allow him the use of a specially designed Braille-type template in the 2002 congressional elections. The complaint, filed in conjunction with the ACLU on behalf of 20,000 blind or visually impaired people in Baltimore County, MD, alleges violations of both the Constitution and the *ADA*.[68] Litigation and settlement negotiations remain ongoing.

Class action suits have also been filed in Florida, Pennsylvania and Texas, and although the plaintiffs have been met with limited judicial success, the overall outcomes of the litigation have been a positive step in gaining equal standing for disabled voters. For instance, Pennsylvania officials are currently negotiating a settlement, which, similarly to the DC settlement, will see election officials supplying e-voting systems to aid disabled voters. Moreover, even though the plaintiffs in Texas lost their case at the appellate level, the state subsequently passed a law requiring that any new voting system purchased must make secret ballot provisions available for blind and physically impaired voters. Thus far, the only state refusing to capitulate to the disabled voters' demands is Florida. Litigation remains ongoing in Florida,[69] and even though a new state statute requiring that any new voting system purchased must be accessible to visually and physically disabled voters, state officials refuse to settle the case until the federal government provides the promised funding to aid in the transition to e-voting.

The clear trend in the U.S. indicates that states will have to provide disabled-accessible voting options or else face the cost and, more importantly, the embarrassment and electoral backlash of defending the discriminatory voting system in court. States are starting to realize the

---

67. Kris Wise, *Voting System to Change: County Moves Ahead Without Guarantee of Federal Funds*, Charleston Daily Mail (Mar. 3, 2003) (stating West Virginia has allocated $3 million of the $10.5 million federal grant for election reform to be used to purchase handicapped-accessible voting machines). *See also* Bryan Mercurio, *Discrimination in Electoral Law: Using Technology to Extend the Secret Ballot to Disabled and Illiterate Voters*, 28 Alternative L.J. 272 (2003).

68. *Poole v. Baltimore County & Md. Bd. of Elections*, No. 02-3610 (D. Md. Election Day 2002).

69. *AAPD v. Hood*, No. 3:01-CV-1275-J-21TJC, (M.D. Fla. 2002). The Florida litigation was filed in Duval County, where there are currently only three disabled-accessible machines in the county for use by the 40,000 disabled voters in the county. It is estimated that a complete fit-out of disabled accessible machines in Duval County would cost only $U.S.900,000. Alan Fisk, *People with Disabilities Are Suing States on Voting*, <http://www.aapd.com/dvpmain/elreform/suestatesvoting.html> (April 18, 2003) [hereinafter *People with Disabilities*]; *See* Cathy Willoughby, *Hanging Chads Could Prove Costly*, <http://www.advertiser-tribune.com/text/n030603a.html> (Mar. 6, 2003) (quoting the Chairman of the Senecca County Board of Elections (Mr Wayne Hoover) as stating "(new voting methods) have to meet all ADA (Americans with Disabilities Act) requirements").

importance of this issue and, as we have seen, are beginning to voluntarily mandate the purchase and availability of accessible voting equipment. This trend is only likely to increase.

C. RELIABILITY AND INTEGRITY

Critics of Internet voting often belabor the perceived security concerns with Internet voting, such as the potential of ineligible voters casting ballots, voters fraudulently casting more than one vote, or hackers erasing or changing election results.[70] Not only is that tactic unproductive, but the criticism is unsubstantiated and the comparison illusory. The risks of Internet voting cannot be simply stated, but must be compared to the current methods of voting available. When compared, it becomes clear that the current system is not a 100 percent reliable, trusted, and accurate electoral system, but a system that revealed its true identity in the 2000 Presidential Election, an election which brought us lost ballots, pregnant chads, confusing butterfly ballots, dubious hand recounts, and impartial electoral officials making important systemic decisions.[71] The current system is depriving millions of Americans of the right to vote or have their vote count equally under our democracy. For that reason, we must study other methods of voting in the hope that they can improve upon our decrepit, ill-administered, and failing system.

1. *Voting Technology: Current System*

It can be said with substantial certainty that the current voting technologies do not produce accurate results. The cause of this problem is debated, but it appears a majority of the problems associated with the election process are not the result of fraud or corruption but are the result of long-term neglect and mismanagement.[72] The electoral system has never received an appropriate amount of funding and consequently, has become outdated and unreliable. The decentralized nature of electoral administration has also played a large part in spoiling the system, with a divide clearly present between wealthy counties and their poorer counterparts.

The recent Cal Tech-MIT study found that punch cards perform the

---

70. Lee Dembart, *Are Internet Ballots a Vote-Fixers Dream*, Int'l Herald Tribune (Apr. 28, 2003).

71. *See e.g.* Mike Clary, *Jeb Bush Testifies on Hands-Off Role in Election*, L.A. Times A20 (Jan. 12, 2001); *A Modern Democracy*, *supra* n. 43.

72. This claim is substantiated by a recent study that shows evidence of fraud is minimal. The study recommends, among others, that electoral authorities upgrade technology and require ID to be shown at the election booth. Lisa Minnite & David Callahan, *Securing the Vote:An Analysis of Voting Fraud* 37-38, <http://www.demos-usa.org/demos/pubs/Securing_The_Vote.pdf> (last updated May 20, 2003).

worst among electoral technologies.[73] The study reported, "voting technologies are not neutral with respect to recording votes cast by voters on Election Day" and concluded that "lowering the rate of error attributable to voting technologies will improve the legitimacy of American elections, at home and abroad."[74] These statistics reveal the wide degree of methods available to voters and also show the varying degree of certainty allowed by our electoral administrators. Unfortunately, since voting administration is still left in the hands of state and local officials, the majority of the precincts relying on poor voting technology are in predominantly minority areas.

While federal voluntary standards for voting equipment were adopted in 1990, existing equipment is exempt; therefore, several poor precincts still use antiquated, unreliable voting methods.[75] Thus, even though the National Bureau of Standards (now the National Institute of Standards and Technology) recommended in 1988 that punch-card voting be abandoned, many jurisdictions took no action and punch-cards remained in over 500 U.S. counties.

Even though punch-cards were the source of much of the trouble in Florida 2000, they remain in use today in many counties.[76] In fact, six different varieties of punch-cards are used across the country's 3,141 counties and 10,000 local jurisdictions, as are five different types of lever-arch machines (including the 38 year old model needing 27,000 parts to operate as used in New York City),[77] ten varieties of optical scanning systems, six types of touch-screen voting, and numerous other forms of voting technologies in various jurisdictions. In the 2000 elections, U.S. electoral jurisdictions relied on twenty-eight different voting methods, with 37.4 percent of the precincts using some form of punch-cards, 24.7 percent using optical scanners, 21.8 percent using lever-arch machines, 7.3 percent using touch-screen technology, and three percent using traditional paper ballots.[78] Not only does the lack of standardization confuse the voting public, but it also results in a different percentage of cast and uncounted ballots in each jurisdiction, potentially violating the right of each voter to have their vote count equally.

---

73. Ansolabehere, *supra* n. 3, at 27-28. Over 3.7 million ballots were cast with punch card voting in the 2000 Florida election. Schwartz, *supra* note 43, at 634.

74. Ansolabehere, *supra* n. 3, at 27-28.

75. "Long-term neglect introduces so many errors into voting and counting ballots that it is impossible to know after an election exactly what the totals are and how many people may have been robbed of their votes." *A Modern Democracy, supra* n. 43.

76. Schwartz, *supra* n. 42, at 634.

77. In 1998, eight percent of the 6,221 lever-arch machines in New York malfunctioned on Election Day. *A Modern Democracy, supra* n. 43.

78. Michael A. Hiltzik & Greg Miller, *Fiasco Reveals a Ballot System Full of Holes*, L.A. Times, A1 (Nov. 11, 2000).

Perhaps more troubling is the performance of some of these voting methods. The 2000 Presidential election revealed the true extent of the damage that flawed ballots and voting methods can do to an election. In Palm Beach County, Florida, faulty ballots appeared to be the reason that over 19,000 votes were deemed invalid. Moreover, faulty ballots have also been blamed for Reform Party candidate Pat Buchanan receiving an inordinately high number of votes in that heavily Democratic county.[79] Statistical analysis estimates that 2,865 of the 3,407 votes cast for Buchanan were actually intended to be cast for Vice President Gore.[80] In an election decided by around 1,000 votes, an election, which ultimately decided the next president, one can clearly link the faulty ballot to the ultimate outcome of the election.[81]

Prior to the 2000 election, the low cost of punch card voting helped keep it popular with electoral administrators despite its propensity for inaccurately rejecting votes where the back of the "chad" is left hanging instead of being fully punched out. In such cases, even though the intent of the voter is blatantly clear, the machine rejects the vote as invalid and, in the event of a recount, partisan officials are left to debate the legitimacy of the ballot.[82]

Not even offline e-voting machines have escaped the voting technology criticism brought about by the 2000 electoral failure.[83] For instance, e-voting machines were initially blamed for leaving uncounted votes in the 2002 Florida congressional elections, but election officials quickly realized that the majority of errors were actually caused by workers either forgetting to plug the storage disk (the disk that records and stores the vote totals) into the computer at the start of voting or forgetting to take the voting cartridge out of the computer after the close of polls (leaving the votes from those machines uncounted). Eventually, untrained workers and election administrators were appropriately blamed for the er-

---

79. The ballot design resulted in several lawsuits by those claiming to be deprived of the right to vote. CNN News, *Congressman Says 19,000 Votes Invalidated; 2 Suits Filed Over Irregularities*, <http://www.cnn.com/2000/allpolitics/stories/11/09/palm.beach.votes> (Nov. 9, 2000).

80. *See* Indiana University Web site of Professor Burt Monroe, located at <http://www.indiana.edu/~playpol/pbmodel.pdf> (accessed January 31, 2003); Online Journalism R., *A statistical analysis of the Florida Vote*, <http://www.ojr.org/ojr/ethics/1017962655.php> (Nov. 9, 2000).

81. CNN News, *supra* n. 79.

82. Optical scan machines also face a similar problem, as these machines require voters to carefully fill in ovals, arrows or boxes and the machine rejects votes which are Xed or checked instead of filled. While some counties allow for election workers to enhance the original in an attempt to clarify the intent of the voter, such interference by partisan election officials can raise the appearance of impropriety.

83. The HAVA allocates more than $1 billion for the purchase of e-voting systems, but numerous technologists have questioned the swift move towards the new voting method. Sam Lubell, *To Register Doubts, Press Here*, N.Y. Times (May 15, 2003).

rors. Despite their performance in recent elections,[84] some information technology experts assert that offline e-voting machines are unsafe and vulnerable to malfunction.[85]

The above analysis of the current voting technologies reinforces Cal Tech-MIT's poignant conclusion that "Americans' votes are not all counted the same."[86] Internet voting at the polling station and remote Internet voting will help correct the inequality, which inevitably stems from the disjointed nature of the American electoral process.

2. *Internet Voting Can Improve the Accuracy of the Vote*

Prior to 2000, the accuracy of election results was rarely investigated. But the 2000 presidential election changed the course of American electoral history. It is estimated that faulty voting equipment and the lack of guidance and instruction to non-English speaking voters, resulted in approximately two million lost or uncounted ballots in the last presidential election.[87] Moreover, several incidents of minorities being intimidated or otherwise discouraged from voting, incorrect lists of ineligible voters, and polling stations either opening or closing at incorrect times served to disenfranchise even more voters.[88] In total, it is estimated that six million voters who intended to vote in the 2000 election but could not vote due to voting machine failure, inaccessibility of polling stations, or incorrect registered voting lists.[89] Since 2000, we have been bombarded with reports of lost, uncounted, or misconfigured votes, of people being

84. Kellie Patrick, *Cartridge Problem Casts Pall on Voting,* Sun-Sentinel 1A (Mar. 12, 2002). While e-voting machines have generally performed without interruption, there have been instances of malfunction. *Id.* However, the majority of the malfunctions have been attributed to human error. *Id.*; *Machines lose 294 early votes - -Software glitch means Wake voters will get re-vote,* N.C. News Observer (Oct. 31, 2002).

85. Dan Keating, *New Voting Systems Assailed,* Wash. Post A12 (Mar. 28, 2003) (reporting that the e-voting systems operating in Maryland "performed flawlessly" and that voters were "happy with how they operated").

86. Ansolabehere, *supra* n. 3, at 29.

87. *A Modern Democracy, supra* n. 43. Voters of non-English speaking backgrounds have uniformly praised e-voting's ease and guidance. Kathay Feng of the Asian Pacific American Legal Center summed up their position by stating "[v]oters who cannot read English well – including seniors and immigrants who may never have used an ATM – have tried these machines out and love them. Electronic voting allows voters to choose their language from the first screen and to see the instructions and their ballot choices entirely in their language of choice. For diverse California, millions of voters will be fully enfranchised because of this bilingual option." California Voter Empowerment Circle, *supra* n. 64.

88. For instance, many voters in Cleveland's predominantly minority east side were disenfranchised when the city relocated the polling booth without notifying voters. *A Modern Democracy, supra* n. 43.

89. Ansolabehere, *supra* n. 3, at 3; *Voting Reform Projects Creep Forward,* Daily J. 7 (July 12, 2001); The Center for Voting and Democracy, *newsletter,* <www.fairvote.org> (Feb. 14, 2003).

disenfranchised or otherwise impeded from voting, and of partisan electoral officials deciding the legitimacy of a vote without a strict standard on which to base their decision. There can be no doubt that the current system disenfranchises Americans.

Internet voting has the ability to correct some of the injustices currently embedded into the system and substantially improve the electoral process. For instance, Internet voting eliminates the human error or prejudice associated with the current electoral system. The 2000 Presidential election so vividly reminded us that partisan electoral officers often act in a partisan manner. The inconsistent, unbalanced system of recognizing and discounting invalid votes seen in that election could not be repeated in a computerized system of voting.[90] Moreover, a fully functional Internet voting system is unquestionably accurate, thereby reducing the instances of losing candidates questioning the count, requesting a recount or otherwise lengthening the process in close elections.

As well as removing bias and human error from the process of determining voter intent, Internet voting adds recognizable standards to the recording and tabulating process. Both polling station and remote Internet voting can enhance the recording and tabulating stage of an election for a number of reasons. First, computerized voting is easy for the voter to understand, resulting in a substantially lower rate of invalid votes. E-voting's rate of invalid votes is consistently under one percent, compared with the large rate of invalid votes that exist under other forms of voting (consistently around five percent).[91] This low rate of invalid votes is due to the design of e-voting systems, which attempts to ensure that the voter properly casts his or her ballot by leading the voter through the process and confirming that the selections the voter made are the ones he or she intended to make.[92] Moreover, e-voting systems allow voters to check their ballot before sending it through (i.e. placing it

---

90. The seemingly standard-less recount resulted in both candidates gaining a considerable number of votes, with Vice President Gore receiving more votes than now-President Bush. CNN News, *supra* n. 79.

91. For example, in Riverside California, where touch-screen voting is used, the rate of invalid votes is negligible, compared to their former system using the punch-card system, which resulted in a large number of votes for multiple candidates. Manjoo, *supra* n. 40. The offline Australian trial resulted in an invalid rate of .57 percent, compared with 4.32 percent of paper votes being deemed invalid. Australian Dept. of the Parliamentary Library, *Electronic Voting in the 2001 ACT Election*, Research n. 2001-02, No. 46 (June 18, 2002) ("Parliamentary Report").

92. Some voters often use the ballot as a form of protest, so the system must be designed to ensure the ability to cast an invalid vote remains possible so as not to curb political speech.

in the box).[93]

Internet voting also has the ability to tabulate and report election results immediately following the close of the polls. As the media increasingly use technology and opinion polls to predict election outcomes before their conclusion, the importance of quick election results have never been so crucial. However, short of a ban on such "speech," the electoral system risks being compromised by overambitious news reporters if it cannot quickly tally and report the voting results.[94] By allowing the media the opportunity to predict election results (regardless of their accuracy), the system risks diminishing the importance of voters in the pacific time zone, who may be discouraged from going to the polls and voting when the Presidential election appears to already have been decided. The electoral system cannot ignore this reality and must actively attempt to eliminate this growing problem.

Another reason to favor the implementation of Internet voting is the current system's failure to authenticate a substantial portion of the votes due to increased absentee voting and relaxed identification qualifications when registering to vote or casting the ballot.[95] Internet voting has the ability to reverse this trend and properly authenticate votes and guarantee that a voter does not cast multiple ballots.

Absentee voting is extensively used in every state to supplement polling station voting, with Oregon entirely replacing traditional voting with a system entirely based on postal voting.[96] In absentee voting, elec-

---

93. This mechanism for checking the ballot could simply be done by a pop-up box appearing which states something of the following nature, "You voted for X. Are you sure you want to vote for X? If Yes, click ENTER. If no, click BACK."

94. In Canada, a British Columbia provincial judge ruled section 329 of the Canada Elections Act, which prohibits reporting vote tallies before polling closes, an unconstitutional infringement of the freedom of expression clause in the Charter of Rights and Freedoms (the equivalent to the American Bill of Rights). Terri Theodore, *B.C. Judge Strikes Down Portion of Elections Act*, The Globe and Mail (Jan. 29, 2003).

95. Six states (Idaho, Maine, Minnesota, New Hampshire, Wisconsin, and Wyoming) currently allow registration on Election Day and, in an effort to increase participation, several other states are considering such a move. Dana Damico, *Registration on Day of Election Considered Backers Say Plan would Draw More Voters*, Winston Salem J. 1 (Apr. 17, 2003). Other states having lax registration requirements often cannot guarantee the authenticity and integrity of their vote. For example, Alaska has 38,209 more registered voters than voting age population and an estimated twenty percnt of Indiana's registered voters are counterfeit and fraudulent. Moreover, in North Dakota, recreational vehicle owners who use the state as a tax haven list campgrounds as their address while also being registered to vote in their "actual" home state. Andrew Nelson, *Voter Requirement OK'd*, Associated Press State & Local Wire 1 (Feb. 27, 2003).

96. While no other state has abandoned traditional voting, counties in several states are considering complete absentee voting for local elections. For example, Pasadena, CA is considering an "all-mail" election, see Pasadena, *City of Pasadena and Pasadena Unified School District Primary Municipal Election* <http://www.ci.pasadena.ca.us/cityclerk/election/2003_defaultsecondary.asp> (Mar. 4, 2003).

tion officials send blank ballots by unregistered mail to the known address of registered voters. Not only does this result in a number of votes being sent to outdated or incorrect addresses, but it also provides easy access for thieves to steal votes from letterboxes or for voters to sell or otherwise allow a proxy to vote in their place. Electoral officials can neither guarantee that the blank ballots reach the proper voter, nor can they guarantee the authenticity of the returned ballot as being from the proper registered voter. In fact, it is estimated that in the 2000 Presidential Election "more than 36,000 of (Oregon's) 1.5 million voters may have mailed in ballots that were signed by someone else."[97] Numerous other states have also recently admitted that serious reliability problems exist within their respective absentee voting systems.[98] Moreover, political parties in some states, most notably Texas, hire so-called "vote-whores" to either steal, pay, or do favors for registered voters in exchange for that person's ballot.[99] Furthermore, voters in many states are not required to show identification before being given a ballot and allowed to vote at the polling station, thereby casting doubt on the authenticity of the final election result.[100]

Opponents of Internet voting cite voter privacy as a reason to oppose the technology, pointing to the fact that outside influences, such as friends, co-workers, family or work superiors, have the ability compel or coerce a voter to vote in a certain way. In fact, it is not hard to imagine a situation where a person voting remotely feels compelled to vote a certain way due to influences of other people in the area where the person is voting. It is also not hard to imagine the even more frightening scenario where voters are voting under duress or coercion, such as a supervisor urging the employee to vote in a certain way with threat of sanction.

While such unfortunate situations cannot be prevented in remote Internet voting, they should not be reasons to oppose the voting method. The same troubling situation is currently present in every state, where voters using the absentee ballots face the exact same pressure and possible coercion that remote Internet voters would face. Postal voting is accepted by the vast majority of voters and electoral officials, yet it is

---

97. *A Modern Democracy, supra* n. 43. An emerging, and yet to be resolved, related problem is that of what to do with existing absentee ballots when a candidate dies or otherwise withdraws from the election before Election Day.

98. *See e.g.* the recent Washington Secretary of State report outlining the problems with that states absentee voting system. Office of the Secretary of State, *Election Procedures Review of King County State of Washington 2002*, <http://secstate.wa.gov/elections/pdf/kingcounty.pdf> (last updated Sept. 24, 2003).

99. *A Modern Democracy, supra* n. 43.

100. States attempting to pass legislation requiring voting-day identification have been met with strong opposition. While the resistance attempts to minimize voter disenfranchisement, it may result in votes being cast by someone other than the proper registered voter.

proven to be victimized by widespread electoral problems, such as lack of verification, undelivered ballots, and vote fraud.[101] Not only does absentee voting escape this line of questioning, but due to its convenient nature, it also enjoys widespread electoral use.

While Internet voting at the polling station would not radically depart from traditional polling station voting (it would only provide as much or as little authentication protection as the jurisdiction currently has in operation under its traditional voting methods), remote Internet voting could provide more authentication and protection than traditional polling station voting through its various security measures, including encryption technology (the scrambling of information during transmission), electronic signatures (the use of passwords and/or personal identification numbers ("PIN,") and biometrics (i.e. digital signatures or digital scan technology) to verify a voter's identity and maintain the integrity of the data during transmission.[102]

D. COST-EFFECTIVENESS

Since the American electoral system is a disjointed unity among the federal, state, and local levels of government, calculating the actual costs of a nationwide presidential election is not a simple task. However, considerable analysis of the 2000 election, including Presidential and Congressional balloting, estimate that the elections cost over $300 million in total. This figure, which does not include certain fixed cost items, including voting equipment, would be apportioned between the federal, state, and local authorities.[103]

Through a combination of lower administrative and training costs and a willingness of software companies to offer package pricing, Internet voting has the ability to significantly lower the cost of elections.[104]

---

101. Oregon laws allow party volunteers to go door-to-door to collect ballots or to drive voters to a postal box to deposit their votes. The recent Oregon election was also plagued with other problems, such as ballots being returned by the post office for insufficient postage.

102. In the Department of Defense trial, voters logged onto the designated Web site and entered their PIN, which had been provided for the trial. Once securely logged onto the site (through PKI technology), voters selected their preferred candidates and completed the voting process. After voting had completed, local voting officials in every applicable county logged onto the site and entered their PIN to retrieve the votes. Officials decided that allowing the system to tally the votes would have been too big a step to introduce in the trial. Therefore, the trial focused on system and security aspects of e-voting. Election officials printed a non-identifying ballot for each voter for the purposes of tallying votes.

103. Ernest Hawkins, *Cost and Finance of Elections*, <http://www.hss.caltech.edu/~voting/hawkins_present.pdf> (Mar. 30, 2001) (paper presented to the Cal-Tech-MIT/Voting Technology Conference).

104. Kevin Coleman, *Internet Voting: Issues and legislation*, Congressional Research Service Report for Congress, Order Code RS20639 at 2 (Nov. 7, 2001).

While the author believes polling station voting should always remain a voting option,[105] the number of polling stations needed during an election could be significantly reduced if a substantial proportion of the voting population chose to cast their ballot remotely, thus reducing the number of polling staff and administrative costs for the electoral commission. Therefore, Internet voting could lower government spending on voting infrastructure and personnel-related costs.

Moreover, remote Internet voting would dramatically reduce, if not eventually eliminate, the need for absentee ballots. This change would substantially reduce the burden of organizing, posting, securing, and counting absentee ballots, as well as reduce the costs of printing and postage. As absentee voting results in several tons of wasted and unused paper, a change to Internet voting would have the ancillary benefit of helping the environment.

Even simply allowing Internet voting at the polling station would ease the administrative burden election officials currently face, as officials would no longer have to carefully supervise the safety, security, and transport of the ballots and instead could concentrate on other pressing matters that inevitably arise on Election Day. Internet voting would also reduce the threat of lost or uncounted ballots, as well as eliminate much of the paper-voting by-product. Counties currently print ballots for all eligible voters, yet voter participation hovers around fifty percent; thus, counties are forced to dispose of the unused ballots after the election. Not only does this waste have a negative effect on the environment, but the printing of unused ballots is also a substantial monetary waste that costs taxpayers money.

While one would assume that developing an Internet voting system would be a time consuming and expensive venture (with initial outlays of developing or purchasing a reliable remote e-voting system, hiring technical experts, and training staff among the many necessities), Internet voting software companies have competitively priced their products with traditional forms of voting.[106] A comparison between a typical voting

---

105. For a similar view, *see* California Internet Voting task Force, *supra* n. 31, at 1; Status Report, *supra* n. 64, at 16.

106. The Reform Party only paid $1 million for Internet voting during their 2000 Presidential nomination process, a figure substantially lower than traditional election costs. Farhad Manjoo, *Reform Voting Evokes E-Votes*, <www.wired.com/news/politics/0,1283,379 64,00.html> (Aug. 3, 2000). While Internet voting cost the Swiss canton of Geneva Swiss slightly more than traditional voting (500,000 Swiss francs instead of 150,000), the figure is expected to decrease with usage. Regardless, these figures are drastically less than some early estimates at the cost of implementing Internet voting, which put the figure as high as $20-$50 million per county. Lance J. Hoffman, *Internet Voting: Not Ready for Prime Time (Yet)* 4, <http://www.cpi.seas.gwu.edu/library/presentations.php> (accessed Jan. 15, 2003).

precinct and a precinct implementing Internet voting illustrates how In-
ternet voting can be more cost-effective than traditional forms of voting.

For the average voting precinct, the rural Missouri county of Greene
will be used. Greene County spent approximately $60,000 for printed
ballots, supplies and delivery in its 1998 presidential primary elections.
This figure does not include the cost of the tabulation machine or initial
purchase of the voting system.[107] In contrast, the city of Oconomowoc,
WI, (currently considering implementing both remote and polling station
Internet voting for local elections) has tentatively contracted with Elec
tion.com to administer its city elections. Election.com would charge only
$16,600 to develop and monitor the system, train city officials, provide
technical support, and certify and evaluate results.[108]

Each county must conduct detailed studies to calculate the short and
long-term costs of Internet voting to ascertain if the system is cost-effec-
tive to implement. However, each county must also realize that, while
retaining the current voting system will be the cheaper in some cases,
the detriments of keeping a failing system could soon far outweigh the
short-term cost savings.

V. DISPELLING THE MYTHS

Millions of Americans use the Internet daily to conduct important
personal, business, and financial transactions. Several key industries,
such as banking, healthcare, and government, also transport private in-
formation in a secure Internet environment on a daily basis. Critics,
however, often cite potential security concerns as a reason for opposing
Internet voting. This section will analyze concerns regarding the credi-
bility and integrity of Internet voting and will not only prove those con-
cerns to be, for the most part, unwarranted, but also that Internet voting
is in fact *more* secure and reliable than numerous forms of voting cur-
rently used.

---

107. When the costs of purchasing election equipment are added to the costs, Internet
voting is even more attractive and cost-effective. Traditional election equipment costs be-
tween $2,000-$11,000 per unit, while a personal computer capable of performing the tasks
required for Internet voting can be purchased for less than $1,000 dollars. Further substan-
tiating the claim that Internet voting will reduce the costs of administering elections are
the statements of Alfred Charles, Internet Voting Task Force Chair and Assistant Secre-
tary for e-Government for the California Secretary of State, who stated that while Internet
voting would cost approximately $6 per vote and traditional voting methods only range
between $3-5 per vote, the savings would be realized in the cost of the voting equipment.
Chernay, *supra* n. 59.

108. Amy Rinard, *City May Conduct Elections on Internet*, <http://www.jsonlin.com/
news/wauk/mar03/122619.asp> (last updated Mar. 3, 2003).

A. ELECTORAL SECURITY

Internet voting systems are designed with numerous security measures to protect the integrity of the election. For example, Internet voting at the polling station can provide measures such as swipe bar-coded cards to activate the computer or biometric identification readers to prevent multiple voting. Of course, while security measures can prevent some voter fraud, they cannot prevent all forms of voter destruction. While the risk of voter sabotage is slight, destructive acts, such as a voter smearing gel on the screen/keyboard/mouse in an attempt to disable the machine or alter votes, could burden election officials and volunteers and may even delay voting.[109]

Some commentators have convinced the public that computerized voting is unsuitable for the voting process because destructive voters hell-bent on sabotaging the election could tamper with or otherwise disable voting machines, but further study regarding potential tampering reveals this argument to be a red herring, as no electoral system is safe from the intentional destructive acts of votes. Indeed, a voter could smash or otherwise disable an e-voting machine, but a voter could just as easily light a match and drop it into the ballot box and destroy paper votes. While both are possible, neither is likely.

Not only is such behaviour not expected of the average voter, but in the event of tampering on a computerized voting machine, it would be on such a small scale as to not affect the results of the election.[110] Moreover, Internet voting allows voters the opportunity to check which candidates they have voted for before registering the vote and correct any errors without losing or altering a single vote. Therefore, if the system were to incorrectly indicate the chosen candidate, the voter would immediately become aware of the problem and report it so that it may be corrected.

Critics have also called the integrity of remote Internet voting into question, pointing to the fact that remote Internet voting does not allow electoral officials to verify that the remote voter is actually the person supposed to be casting that ballot.[111] On closer inspection of this argu-

---

109. In Italy, authorities recently foiled the mafia's plan to control the election result by having voters use their 3G mobile video phones to send pictures of their completed ballots for inspection before casting their votes. BBC News UK Edition, *Mafia Turns to 3G Video Phones*, <http://news.bbc.co.uk/go/pr/fr/1/technology/3033551.stm> (May 21, 2003).

110. For example, critics often claim that e-voting will experience problems such as screen failure due to repeated finger jabbing or barcodes failing to activate machines and while these problems could occur, they are rare and easily discoverable. In most elections, problems the machines have usually have been corrected within minutes of discovering the problem and very rarely does a machine ever have to be decommissioned during an election.

111. *See e.g.* Cynthia H. Craft, *Making Sure that California's Votes Are Actually Counted*, L.A. Times, Opinion, Part M, 1 (Dec. 17, 2000) (California Secretary of State, Bill

ment, one again sees its flaws when compared to the current system of voting. As stated earlier, every state extensively uses postal voting to supplement polling station voting (with Oregon exclusively using postal voting to replace traditional voting). The postal voting process is highly insecure and often leads to blank ballots not reaching the intended voter for a number of reasons, including theft. Electoral officials cannot guarantee that the blank ballots reach the proper voter nor can they guarantee that the authenticity of the returned ballot as being from the proper registered voter. Not only does this disenfranchise the legitimate voter, but it also threatens the integrity of the entire electoral process. The integrity of the current absentee process is also threatened by politically affiliated "vote-whores," who as explained earlier, attempt to buy or steal ballots in order to gain a political advantage for their party.[112]

However, the absentee voting process is not the only threat to the integrity of American elections. Many states have no requirement that voters show identification before being given a ballot and being allowed to vote at the polling station. This allows voters to assume another identity in order to cast more ballots in favor of their preferred candidate.

Remote Internet voting can drastically reduce, if not eliminate, the occurrence of such fraudulent voting practices by requiring identification particulars from voters when they log on to cast their ballot. While no voting system can provide a 100 percent guarantee against all forms of fraud or irregularities, Internet voting attempts to reinstate integrity in the voting process through a number of security measures.

These security measures could be implemented in a number of ways. One such method would require the voter to encrypt the ballot with a secret key before sending it to the election office. The voter would send the ballot, with their blind signature, to a verifier who verifies that the person is a registered voter. If found to be valid, the ballot would be returned to the voter, who would remove his/her identification signature and send the ballot, with the encrypted signature of the validator, elec-

---

Jones, stated, "[we] don't have the ability to verify who a person is on the other end of the PC or the Internet").

112. Other forms of bribes are also commonplace; for instance, a radio personality in Canton, Mississippi was recently investigated after providing a half-bottle of gin in return for votes in the 2002 Democratic primary. *Radio Personality Accused of Exchanging Gin for Votes*, Associated Press (Apr. 18, 2003). Vote hauling has also become a big issue. Vote hauling occurs when supporters pay people to drive other voters to the polls. In one instance, a candidate paid 1,217 people $50 for the service. Incredibly, this service is legal in some states. *See* Rick Hansen, *Vote Buying*, 88 Cal. L. Rev. 1323 (2000). Moreover, California allows payments for convincing people to vote, but state law prohibits the payment being conditioned on voting for/against a certain candidate. This practice has been put to use by the Democratic Party, who targets poor neighborhoods with coupons for free donuts. In Alaska, candidates have been known to use free gasoline coupons as the voting sweetener. *Id.*

tronically to the electoral office. The electoral office would then publish the names of Internet voters for those voters to verify that for all names that are listed, they were the ones who actually voted. The voter then sends the encryption key to the electoral office and the electoral office publishes the encrypted ballot and key for vote verification.

Another possible solution would be to have voters sign up to vote remotely before the election. The electoral office could send those voters a disk containing a cryptographic key and an affidavit, which the voter would sign and return.[113] The encrypted key would only be activated after the affidavit is checked against the voters name on the roll. The actual vote would also be encrypted with a different key to generate an anonymous e-mail.

Yet another alternative to authenticating votes may be to introduce a voter's smart card, which carries the holder's particulars on a microchip in the plastic card and can be used to verify a voter's identity both at the polling station as well as remotely. Such a system has worked successfully in Finland; however, in the short-term, it is impractical to expect that voters have card scanners connected to their computers.[114] Other possible identification techniques, such as biometric authentication devices and cryptographic devices, also suffer the same deficiency.

Unlike the current system in place in many jurisdictions, the above examples would also prevent voters from voting twice and reduce the instances of fraud, as the security system would not allow the voter's identification information to be opened and accessed more than once. The above examples also prove that it is feasible to provide voters the chance to cast their ballot from anywhere in the world while also surpassing the level of authentication and uniqueness currently available in many current voting technologies.

Due to the problems with postal voting and people voting at the polls without providing identification, one can feasibly argue that Internet voting is actually *safer* and *more secure* than postal voting and some polling station voting. This assertion is backed by the California Internet Voting Task Force, which reached the conclusion that "it is technologically possible to utilize the Internet to develop an additional method of voting that would be at least as secure from vote-tampering as the current absentee ballot process in California."[115]

---

113. The disk would be secure so that it could not be numbered to track the voter and how the voter cast their ballot.

114. Symposium, *Technology and Administration in Election Procedure,* SOU 2000:125, 5.2 (2000) (Swedish Ministry of Justice) [hereinafter "Swedish Report"].

115. *California Internet Voting Task Force, supra* n. 31, at 1.

B. AUDITABILITY

Many Americans have been led to believe that the paper trail for verification, commonly called the "audit trail," is removed from all forms of computerized voting. The removal of such auditability is troubling for a number of reasons, not least of which is the inability of electoral officials to verify that all the votes have been accounted for in the final tally. However, the widely held view that computerized voting completely removes the "audit trail" from the voting process is misleading.[116]

While it is true that Internet voting trusts computers and voting software to properly record, forward, and tabulate the votes, software companies insist that polling station e-voting systems prevent against vote loss. Further, an audit trail is created, by sending and burning every transaction on the server to a CD, which would serve as a back-up in the event of a hardware problem or total malfunction.[117] The companies also assert that their voting systems utilize an algorithm that mixes up the order in which ballots are stored on the server, thus ensuring that the vote of each voter cannot be traced back to that person and preserving the secrecy of the ballot.

Even those voters who view the software companies' claim of creating an audit trail with suspicion cannot doubt the ability of Internet voting at the polling station to resolve the problem with a print-out of the paper ballot. The ballot could be internally stored or printed out for the voter to place into a special voting box. In the event of electoral doubt, election officials could check the accuracy of the system by manually counting the paper ballots. This satisfies the need for some to have a paper trail and also allows election officials to closely scrutinize the voting system.

Such as system is in operation in Brazil, where the entire election is now conducted using offline ATM-style e-voting technology.[118] In Brazil, after a voter completes the voting process, the machine prints a receipt located behind a Plexiglas covering which the voter can view. The receipt

---

116. The issue of auditability came to the forefront of debate in early-2003, when the Santa Clara election board voted 3-2 to spend $20 million to purchase offline e-voting machines without a printed audit trail. The board negotiated to have printers installed at no cost should it see the future need. Critics of e-voting had used this as a test case to lobby against such machines. *Silicon Valley Wary of Voting Machines,* N.Y. Times (Feb. 25, 2003); Aron Goetzl, *Proponents of Audit Trail Technology Garner Mixed Results In Santa Clara,* <http://www.electionline.org> (Feb. 27, 2003).

117. Unfortunately, such a system is not available in remote Internet voting and there is no way presently known to create a paper trail during remote voting short of attempting to have every voter print a receipt and send it to a central location. Status Report, *supra* n. 64, at 9.

118. Brazil phased in e-voting, first implementing it in local elections (1996) before introducing it to most federal electorates (1998) and finally the entire population (2002). *See* Brazilian Electoral Office, <http://www.tse.gov.br>.

indicates which candidates the machine has registered the votes for and allows the voter to cancel out the votes and vote again if necessary.[119]

On the other hand, having the voting machine print "receipts" could potentially create more problems than it solves for a number of reasons. First, printing a receipt adds further administrative and monetary burdens to the voting process. Moreover, the addition of printers is likely to create a plethora of Election Day problems. Procedures would have to be in place in the event of printer failure or malfunction and administrators would have to guard against the possibility of printers running out of ink or paper. Procedures would also have to be put in place in the event of a voter claiming the printer did not accurately reflect how the voter wished to vote, yet the vote was cast regardless. For these reasons, the printer-related precaution, if adopted, should only be used in trials and phased out as voters grow confident in the technology.[120]

The 2000 Presidential election revealed that the current electoral system is fraught with errors, inconsistencies, and uncertainty. The painstaking process of manually counting and re-counting the ballots in order to reach an election result (which may or may not have been accurate and complete) showed many Americans the chaotic nature of such a system. This need not be the case, as Internet voting can bring stability and integrity back into elections and so that election results accurately reveal the intentions of the voters.

C. SECURITY CONCERNS

Americans now rely on the Internet for both work and pleasure, and collectively, more than 100 million Americans annually spend more than twenty-eight billion dollars (as of 2000) through e-commerce and web purchases, money transfers, bank transactions, and stock purchases.[121] So why do some Internet users frown upon using the technology to assist the fledgling electoral process when existing security measures adequately protect Americans who transact over the Internet?

The answer apparently lies in the need for the electoral process to get the entire election correct the first time, every time. While e-commerce has a good track record for security, we realize and accept that

---

119. Approximately three percent of the paper-ballots are checked against the recorded votes to ensure the accuracy of the system. Holli Riebeck, *Electronic Voting in the Amazon*, <http://www.spectrum.ieee.org/WEBONLY/wonews/oct02/brazil2.html>.

120. A former electoral administrator claimed, "(having a printer installed at the polling machine) would create a lot more problems then it solves." *Silicon Valley Wary of Voting machines, supra* n. 116.

121. Keith Regan, *U.S. Online Spending Up 62 Percent in 2000*, <http://www.ecom mercetimes.com/perl/story/7537.html> (Feb. 15, 2001).

some level of fraud exists in Internet transactions.[122] Electoral systems do not have that luxury. Even a small hiccup in a voting system could cause irreparable harm to the electoral system and democratic process. The 2000 Presidential election proved that minor procedural deviations combined with electoral oversight could quickly turn an advanced electoral and democratic system of a highly sophisticated nation into a tangled fiasco.

For that reason, software companies have provided numerous safeguards protecting the electoral process from security breaches. These necessary safeguards create a fundamental trade-off between the convenience of the voter and the security of the voting system. As convenience is added to the electoral process by allowing people to vote remotely, security of the vote is reduced; thus, as security measures are increased, some of the convenience associated with Internet voting dwindles.[123]

Security breaches have the potential to irreparably damage an election and can occur in two ways: (1) by an attack that targets the client or server directly, commonly called a penetration attack; or (2) by an attack that targets and interrupts communication between the client and the server, commonly called a denial of service.[124]

1. *User and the Server*

Penetration attacks occur when a hacker transports a virus to its target by one of a variety of mediums, including floppy disk, CD-ROM, download, e-mail or by exploitation of an existing bug or security flaw in the targets computer or browser. Penetration attacks are a common occurrence and difficult to defend against.[125] Once the virus is transported and in place, the hacker can do as he or she pleases and could easily spy on users casting their ballots, prevent users from casting their ballots, or

---

122. Ed Gerck, *From Voting to Internet Voting*, The Bell 1, 5 (2000) (Gerck estimates ten percent of transactions are the subject of fraud); Craig Bickenell, *Credit Card Fraud Bedevils Web*, <http://www.wired.com/news/business/0,1367,18904,00.html> (Apr. 5, 2002) (Bickenell states five to six percent of Internet transactions are fraudulent).

123. Such security measures, which could impact upon the convenience of voting include having voters pre-register for online voting, sending a CD-Rom to voters to install and/or sending a password and PIN number to the voter. Richard M. Schum, *Internet Voting: Its Perils and Promise*, <http://www.netvoting.com> (May 9, 2002); David Elliott, *Examining Internet Voting in Washington*, State of Washington White Paper 4 (May 3, 2002) (available at <http://www.electioncenter.org/voting/InetVotingWhitePaper.html>).

124. Avi Rubin, *Security Considerations for Remote Electronic Voting Over the Internet*, <http://www.avirubin.com/e-voting.security.html> (Jan. 11, 2003) (detailing Internet security considerations).

125. *Id.* at 2-3. There have been numerous well-documented instances where hacking has damaged or delayed major computer systems, including Yahoo, Hotmail and U.S. government sites. *See e.g.* The Centre for the Study of Technology and Society, <http://www.tecsoc.org>.

even modify a voter's ballot.[126] Even worse, the hacker can accomplish all of the aforementioned activities without the voter's knowledge or detection from security measures such as encryption devices or anti-virus software.[127]

A successful remote Internet voting system must also protect against a plethora of other hacker activities, including "man in the middle,"[128] "page jacking,"[129] or similar disruptive and highly damaging attacks that could be aimed at voters on Election Day.[130] These types of attacks pose the same risks as other infiltration attack methods, yet are much easier to carry out. Further, most encryption technologies cannot guarantee success against a potential breach.[131]

Voting experts feel that hacker-related security risks can be neutralized and that Internet voting could be at least as safe as the current system of absentee voting. Some experts even conclude that, if administered appropriately, "Internet elections could pose less risk than traditional elections."[132] This conclusion is based on the fact that current security measures, such as Secure Sockets Layer ("SSL") technology, have proven themselves to be safe means of transporting information over the Internet. SSL technology is the most widely used method by e-commerce sites for submitting credit card information to process sales and by banks to process account numbers, balance inquiries and money transfers. SSL creates a confidential communications line between two computers and encrypts the data as it is sent through the line, thereby protecting it from outside interference. Security breaches with transmissions protected by SSL have been deemed a "pretty marginal problem,"

---

126. A trojan horse virus can be activated at any time after delivery, including remotely, by timer, or by the detection of certain events by the host (or a combination of the above).

127. Encryption devices are only effective if they commence protection before hackers gain access to the system. Moreover, even if the device successfully commences protection, this kind of attack can target an area of the computer, which is not protected (encryption protects only the operating system and browser). *See* IPI Report, *supra* n. 9, at 13-14.

128. *Id.* Man in the middle occurs when a hacker misleads the user into thinking they are on the correct Web site when in fact they are on the hacker's site. The hacker collects the information entered by the user for later fraudulent use while the user believes they have successfully completed their business on the proper site.

129. *Id.* Page jacking occurs when a hacker leads a user off the intended Web site and onto an impostor Web site. Once on the impostor site, the users browser is disabled and the user is shown advertising or other information. The user then has some difficulty in accessing their intended Web site due to the blocks presented by the hacker.

130. *Id.* One example of another method used by hackers is "spamming," which floods the system with requests to prevent the authorized user from responding to legitimate requests.

131. *Id.* at 16.

132. Cherney, *supra* n. 59 (citing Sam Diaz, *Arizona Democrats Can Vote Online in Primary*, Knight-Ridder Trib. Bus. News (Mar. 3, 2000)).

that tends to arise more with public terminals than home systems.[133] However, software companies can provide even more security measures to prevent fraudulent votes or hacker attacks by installing such measures as public key infrastructure ("PKI"), smart-card readers, biometric authentication devices, and cryptographic devices.

In contrast, Internet voting at the polling station is inherently less susceptible to outside hacker attacks and considerably safer than remote Internet voting because election officials control the server and voting software at the polling station. With reliable technology and support to administer the voting system, it can easily be configured to prevent Internet communication with any outside server as well as prevent disgruntled workers from installing any additional software onto the machines.[134]

Both polling station and remote Internet voting have endured several trials and have not suffered from any electoral failure. The success of the security systems protecting the trials is encouraging, but software designers must constantly upgrade the system to prevent any possible element of intrusion.

2. *Denial of Service*

Election officials must also ensure that the path between the user and server is secure. Providing a secure transmission requires an authenticated line between the user and server as well as the encrypted transportation of data along that line. Current technologies can ensure the latter through encryption technology (such as PKI). However, maintaining the authenticated communication link between user and server is a much harder proposition.

Denial of service attacks focus on the path between the computer user and the server. A hacker effectuates the attack by overloading a Web site with requests for information, thus "jamming" the lines and preventing others from using the site.[135] Currently there is no way to stop the "jamming" without shutting down the system and thus shutting out legitimate users until the diagnosis and network administration is completed.[136] Before implementing Internet voting, election officials

---

133. *Id.*

134. As opposed to the open system used in remote Internet voting, online polling station voting uses a closed network system, where the voter's interface is not accessible remotely, thereby eliminating the threat of hacker attacks.

135. Daemons can be installed on a user's computer, without that user's knowledge, to perpetuate the attack against a server or site.

136. Such an attack took place during the Canadian New Democratic Party (NDP) leadership convention on Jan. 25, 2003. The attack shut out legitimate users for 45 minutes before the system could be corrected. *Computer Vandal Delays Leadership Vote*, <http://www.cbc.ca/cgi-bin/templates/print.cgi?/2003/01/25/ndp_delay030125> (Jan. 25, 2003).

must ensure that the path between the computer user and the server cannot be illegally beached.

Moreover, election officials must be able to guarantee with some certainty that their computer server will be able to effectively handle the amount of Internet traffic created by large groups of people attempting to vote at the same time. This problem, commonly referred to as a "bottleneck," is similar to jamming except that it is caused by an overwhelming number of legitimate users. As many Internet Web sites get millions of hits per day,[137] this aspect of remote Internet voting should not be too much of a problem with proper technical support.[138]

Even though the likelihood of denial of service attacks and bottlenecks on polling station voting is minimal, the threat can be avoided entirely by designing a system, which allows voting to continue even if the line of communication between the precinct and the server is lost. In essence, to ensure the system is safe, the system switches to a direct recording electronic (DRE) mode without losing a vote.[139] Using DRE, votes would be recoverable even if the online system were corrupted beyond repair. Unfortunately, this fallback-system of DRE is only compatible with Internet voting at the polling station, as it is not feasible to implement DRE on every remote computer.[140] Remote Internet voting must therefore depend upon election officials providing the needed security to maintain a clear line of communication between the voter's server and the central server, much like the absentee voter has to rely on the U.S. postal service to maintain efficient and secure service to transport the ballot to the election office.

The task of election officials developing, controlling, and maintaining a properly functioning and secure site to allow Internet voting is certainly feasible. In fact, the Swedish Internet Committee concluded that

---

137. One of the most visited Internet Web sites, CNN, gets 230,000 hits per minute on a slow day and can get more than 2 million hits per minute during breaking news. Volera, *CNN Delivers Unprecedented Online Service*, <http://www.volera.com/corporate/pressroom/casestudies/cnn.html> (Jan. 8, 2003).

138. Some commentators claim the "traffic" problem can be avoided by allowing voting over multiple days. While this system effectively operates with the postal voting, multiple day voting has the potential to significantly effect the political advertising campaign of the parties and may lead to situations of bribery or votes for favors.

139. DRE essentially operates as an offline, computerized e-voting system, where votes are recorded, stored and tabulated electronically. For more analysis of offline, e-voting, *see* Bryan Mercurio, *Electronic Voting: Benefits and Burdens*, 2002 Electoral Law Conference (Dec. 6, 2002).

140. Leaving aside the financial and logistical costs of implementing DRE on personal computers, it would be unacceptable for election officials to rely on voters to store and transmit their vote in the event of a denial of service attack. Thus, in remote Internet voting, the reliability of the communication between the computer and the server as well as maintaining a functioning back-up server is much more critical.

various security measures "fulfill reasonable requirements for a secure system."[141] The California Internet Task Force, while recognizing there are "significant" threats to the security and secrecy of Internet voting, concluded the Internet could be used to develop a system which would be at least as secure from vote-tampering as the current absentee ballot process.[142]

VI.   OTHER CONSIDERATIONS

A.   CULTURAL CONSIDERATIONS

While social science issues are more abstract than security or cost-related concerns, the effect of Internet voting on the community must be considered before implementing Internet voting. While Internet voting at the polling station would have a minimal effect on the voting culture,[143] the advent of remote Internet voting on a widespread scale could affect the voting culture quite substantially.

Opponents to remote Internet voting claim that its implementation has the potential to destroy the social cohesion of voters and produce the negative result of a divided society. Traditional voting is seen to promote the community over the individual, where the civic duty of voting is ritualistically followed by all citizens, citizens whom for one moment in time enjoy equal standing of all others, regardless of situation, wealth, color, beliefs, or education. On the other hand, if one segment of society opts to vote remotely instead of physically going to the polling station, the community ideals formed by voting are seen to disappear.

Recognizing there is some idealistic merit to the above argument, a move to online voting would have to be done in such a way as to not diminish or undermine the significance of the event and the sense of community that voting creates. The above argument, however, counters the modern trend of relaxing voting rules to encourage participation and should not be an absolute bar to implementing remote Internet voting. Voters are increasingly using the absentee ballot to cast their votes, even when they do not have a legitimate excuse for not turning up at the polling station. In fact, political strategists and scholars estimate that more than 15 percent of the vote is now cast before Election Day.[144] Moreover,

---

141. *See* Swedish Report, *supra* n. 114, at 5.2.

142. *California Task Force on Internet Voting, supra* n. 31, at 1.

143. Voters would still travel to the polling booth to vote, but would vote via a computer terminal or touch-screen machine as opposed to a pencil and paper. However, any form of voting needs to have the voters' confidence, meaning issues regarding computer tabulations, malfunctions and the lack of an audit trail (all of which are discussed earlier) would figure into the issue of voting culture.

144. Adam Nagourney, *Early Voting Puts Many candidates in Early Overdrive,* <www. nytimes.com/2002/10/14/politics/14ELEC.html> (Oct. 14, 2002).

as mentioned earlier, Oregon has now adopted an all-postal voting system, thereby completely destroying the social cohesion polling station voting attempts to bring to the community. Therefore, allowing remote Internet voting to supplement the current system will only add convenience and encourage greater participation in the voting process in the same way that absentee voting has been doing for years.

Other social arguments against remote Internet voting generally revolve around the ideas that remote Internet voting could trivialize and under-emphasize the meaning and importance of the electoral event. Some opponents of Internet voting insist that voters will not give adequate thought to their choice or to the magnitude of the event if they do it at home, work, or in an Internet café. As many voters have a fair idea of the issues and their preferred candidates before entering the polling station, the fact that a keyboard and screen are in front of them instead of a pencil and paper does not alter the fact that the person still must actively decide what to tick before they leave the corridor. In fact, proponents of Internet voting insist the contrary is true: voters will sit down to vote and use the Internet to research the candidates and the issues before selecting their preferred choices.[145] While the truth may lie somewhere in between the two opposing views, it is unlikely that remote Internet voting will have a dramatic effect on views regarding the importance of the event or on the way Americans cast their ballots.

The effect of remote Internet voting on the election campaign is another area that concerns many commentators. Some advocates of remote Internet voting claim that it could give voters the opportunity to vote over several days, instead of the traditional one-day period for voting. They claim that a multiple-day voting period would add convenience to the process and reduce the likelihood of Internet traffic, which can cause server delays. While the necessity of multiple-day voting is open to debate, the change multiple-day voting is not likely to have an impact on the election campaign if remote Internet voting is only a supplement to, and not a replacement of, polling station voting. While political campaigns are currently designed to end with the culmination of a one-day election, election officials already tolerate a certain amount of early voting in the form of absentee voting. Unless remote Internet voting becomes the norm used by a vast majority of voters, the effect of remote Internet voting on election campaigns is likely to be minimal.

Finally, opponents of remote Internet voting claim that the use of Internet technology will alter the existing structure of our nation's delib-

---

145. Of course, the Internet gives virtually anyone with a computer to "publish." Thus, while information is plentiful on the Internet, the quality and consistency of information is often inconsistent and unreliable.

erative democracy.[146] Our federal framework, complete with separation of powers, sufficient checks and balances against the arms of the government and a bicameral legislature, quite deliberately promotes deliberation over efficiency and substantially limits the excesses of direct democracy. Opponents claim that the advent of remote Internet voting could substantially undermine the system, as the Internet could be seen as an end run to the legislative process and be used to overcome logistical and economic barriers to more frequent elections or referenda. Opponents envision a situation where politicians could threaten the integrity and character of our system of government by seeking to please the electorate or avoiding tough decisions by referring the issue to referendum; this process of direct democracy could lead to frequent referenda in opposition to genuine reflection and would not serve the best interests of Americans.

The chances of such a slippery slope argument towards deliberative democracy being realized are unrealistic. Equality and fairness dictate that all voters must have the ability to cast their ballots. As not all voters have access to remote computers and thus, would not have the ability to cast their ballots in the repeated plebiscites envisioned by opponents of remote Internet voting, this argument really is a non-issue. Moreover, even in the unlikely scenario of a vast majority of voters opting to use remote Internet voting, equality still would mandate that polling stations remain open for those voters not able to use the Internet option. Therefore, the cost and administrative burden of repeatedly organizing polling stations for frequent plebiscites would make this option unworkable.

B. LEGISLATIVE CONSIDERATIONS

Any electoral system built on a weak legislative foundation creates opportunities for electoral challenges and lawsuits. The absence of tangible public scrutiny and a recognizable audit trail could trouble losing candidates and their supporters and may also lead to challenges in the courts. If the recent 2002 Congressional elections can be used as a guide, then, when all else fails, losing candidates will once again rely on the failure of the e-voting system to accurately record votes as an excuse. The argument is rarely valid, as the majority of faults are a result of human error causing the machine to "malfunction," and candidates who initially blame e-voting often quickly abandon such allegations and move onto electoral administration or other reasons to blame for their loss.[147]

While legislation cannot completely avoid such questions, legislation can and must be drafted in such a way to minimize these instances from

---

146. Schum, *supra* n. 123, at 9.
147. For numerous instances of this occurring, *see* <electionline.org>.

occurring. In addition, legislation must be drafted in such a way as to effectively handle disputes and lawsuits that may arise in the course of and following an election.

The prospect of implementing any form of Internet voting requires substantial review and reform of the current electoral laws in light of a changing environment. The current system effectively handles conventional voting offences and abuses but may not be sufficient for new risks posed by the Internet. In order to implement any form of Internet voting, the various federal and state electoral acts would have to be scrutinized to ascertain which sections would need amending to accommodate the technology. For instance, legislation referring to "ballot-papers" or similar references to traditional forms of voting would have to be amended. In addition, provisions relating to a "recount" and events that trigger such an action would also have to be amended and updated for an Internet voting environment.[148] Moreover, it would be imperative to add several new sections to the legislation regarding the tabulation of the votes, such as an amendment banning election officials from releasing voting information until the close of the polls (as the publication of results before other stations have closed could dissuade voters from voting).[149]

In addition, special care would need to be taken in drafting provisions relating to the criminalization of all forms of corrupting or tampering with or attempting to corrupt or tamper with polling station e-voting machines. While some provisions of various electoral acts contain blanket statements against interfering with the electoral process, the accuracy of the machines is essential to the success of an Internet-based election. Therefore, special consideration of the changing environment and stiff penalties would have to be specifically addressed in the legislation.

While the amendments needed to implement Internet voting stations at polling booths appear straight forward, amending the respective Acts to allow remote Internet voting is a more complicated task. For instance, remote Internet voting would mandate the legislation being further amended to prohibit and criminalize a person from stealing, coercing, buying, selling, or giving away their digital signature and/or vote.[150] In addition, the Act, in association with other laws, would have to criminalize all forms of hacking into the voting system as well as jamming or reducing access/spamming the voting system to prevent the offi-

---

148. Other issues which need revisiting include ballot secrecy and privacy issues.

149. Prohibiting officials from even collating the results may be considered to prevent leaks to the press.

150. While anti-bribery laws may arguably already cover such activities, specifically legislating against such activity is recommended.

cials from responding to legitimate requests.[151]

Moreover, amendments must also prohibit persons from page jacking or spoofing sites for the purposes of intentionally deceiving or otherwise impeding the legitimate user in casting their vote. Further, the legislation should also include a section criminalizing the invasion of privacy by attacking a ballot or Web site with intent to examine or change votes.

Another primary concern associated with Internet voting is one of jurisdiction. As the Internet is not controlled by one sovereign entity, but rather an uncontrolled, international medium, the government and election officials need to seriously consider the consequences of implementing remote Internet voting. The law relating to a security breach or act of fraud occurring online due to the act of a foreign national not within the jurisdiction is an unsolved problem. Leaving aside the challenge of even finding the culprit, an overseas, foreign national may not be subject to prosecution within the U.S. without the use of long-arm statutes and extradition treaties.[152] As foreign laws may differ in their criteria for an offence or in their application, the foreign nation holding jurisdiction over the offender may not submit the offender for extradition.

VII. THE FUTURE

Before fully implementing Internet voting, further studies need to take place across a wide range of disciplines. Specifically, technical experts need to improve the Internet voting systems overall, particularly security and encryption technology, so that election officials can safely implement the system for use by the widespread voting public.[153] In addition, political scientists must study the effect of Internet voting on public confidence of the electoral process, the effect on participation and the effect on the character of elections. Finally, lawyers need to analyze the existing electoral laws and develop new laws that ensure that electoral failure does not result from a legal breakdown.

---

151. Again, while electoral acts have provisions banning the intentional interference with electoral administration, specific sections criminalizing this activity is recommended.

152. The use of reciprocal agreements among nations to effect multinational jurisdiction and enforcement actions such as apprehension and extradition of suspects is crucial to successfully implementing remote Internet voting. Failing that, nations will have to rely on international laws to respect the democratic elections and processes of a sovereign nation and protect that nation from incursions, which seek to destroy or undermine security and stability of the democratic process of a nation.

153. Electoral officials would be wise to consider a certification program for any e-voting system. The program should have strict security and reliability standards as well as strong verification of systems. It would also be wise to use pre-existing open source code e-voting systems as models to base improvements. While the use of open source codes may inhabit some intellectual property rights, the trade-off of a more secure system, which is open to public scrutiny far outweighs the negative effect on proprietary rights.

Public trials of Internet voting also must be expanded. Only with experience can election officials gauge how a system works and only with experience can technical experts, social scientists and lawyers assess the strengths and weaknesses of a system and make it a viable option for future elections.[154]

Internet voting trials have thus far been successful and encouraging, yet many remain skeptical of the technology. For this reason, a slow, evolutionary change is needed to introduce Internet voting into our electoral culture.[155] Such change can be accomplished through a gradual introduction of Internet voting accomplished by a two-phase introduction approach. Phase I would utilize Internet voting technology in the existing polling stations by allowing voters the choice of voting at the polling station via the Internet or by traditional methods.[156] Phase II would eventually introduce remote Internet voting to the electorate when the technology is ready and when the voters have sufficient confidence in e-voting systems. This slow, gradual approach would allow for constant monitoring, security, testing and improvements and avoid introducing a radical change that could weaken voter confidence in the electoral process.[157]

Unlike many other nations studying Internet voting, the U.S. has sufficiently laid the initial groundwork for the transition to Internet voting through the public and private trials detailed earlier in this article. Therefore, the next step for Internet voting is its gradual introduction in binding, public elections. The evolutionary approach to introducing Internet voting is not without its challenges or risks, but those potential pitfalls can be minimized through careful planning and implementation. Although Internet voting could be introduced in several ways, below is a list of recommended avenues for its introduction into the American electoral landscape.

---

154. The IPI Report stated trials could be used "to gain valuable experience prior to full-scale implementation." IPI Report, *supra* n. 9, at 2. "The security problems that might arise might well undermine the legitimacy of the electoral process," said David Cheney of the Internet Policy Institute. National Science Foundation Press Release, *Internet Voting Is No "Magic Ballot," Distinguished Committee Reports,* <http://nsf.vov/od/lpa/news/press/01/pr0118.htm> (accessed Jan. 15, 2003). "We must dispel the myths associated with Internet voting and educate public officials to avoid this scenario." *Id.*

155. *See e.g.* California Task Force on Internet Voting, *supra* n. 31, at 2; Status Report, *supra* n. 64; Hoffman *supra* n. 106; Swedish Report, *supra* n. 114, at 5.4.

156. While acknowledging the long-term benefits of remote Internet voting, the IPI report instead recommended Internet voting at the polling, where election officials could maintain control of the security and technology. *Report Pans Internet Voting, supra* n. 30.

157. *See* California Internet Voting Task Force, *supra* n. 31, at 2.

1. *Limited Polling Station Voting*

The first step towards an Internet voting option could the introduction of polling stations for a limited number of voters. This limited trial could take place at select polling stations to test the security, accuracy and ability of Internet voting while providing the voter with more convenience and voting options.[158]

The trial would also introduce the concept of Internet voting to the electorate in a comfortable atmosphere without radically changing the familiar voting surroundings. Over time and with successive successful elections with Internet voting, voters will likely get acclimated to the system and acquire the same level of confidence in Internet voting that they have in traditional voting methods.

In addition to introducing Internet voting to the electorate, a limited-scale trial such as this would attract significant media attention, which, if successfully operated, would generate even more attention and excitement.

2. *Overseas Voters*

American citizens currently living or traveling abroad would be another potential trial market for Internet voting. This option could be implemented in a number of different ways and could be used to trial polling station or remote Internet voting.

One possible trial could simulate polling station voting and give overseas voters the option of voting via the Internet at the selected overseas polling stations (possible locations include the local American Embassy or Diplomatic Mission).[159] Voters would turn-up at the designated polling station and, after clearing the normal identity checks, cast their vote electronically via the Internet.[160]

Another, more advanced option for an Internet trial would allow voters to register as an overseas voter and give them the option of voting remotely over the Internet. In the initial stages, voters would likely be given PIN and CD-ROM (for reasons of security and browser compatibility) but with time other, less intrusive methods could be trialed. Voters would then log onto the voting Web site from any location and cast their ballot via the Internet.

---

158. The trial would be similar to the U.S. Dept. of Defense trial and limited in size and scope to only involve a certain percent of the electorate, which, in the unlikely event of failure, would not have a great impact on the election results.

159. Polling stations could either have hard-copies of the electoral roll or access the roll electronically to verify the voter is eligible to vote and in what jurisdiction.

160. In real-time or once polling has ended, the secure polling station server could send the votes via the Internet to secure servers in the appropriate jurisdiction of each voter.

Another alternative for trialing Internet voting with overseas voters would simply update the current process used for absentee voting, whereby requested ballots would be distributed via secure-email. The voter would then have the choice of returning the ballot via secure e-mail or printing out the ballot and returning it, along with their signature for verification, via the post.[161]

VIII. CONCLUSION

The 2000 Presidential election proved that the current voting systems used in the U.S. are not sufficient to maintain the level of integrity required in a sophisticated democracy.[162] Equipment once thought-off as near perfect electoral aids, such as the lever-operated machines and punch cards readers, in fact could and have become highly contentious and undesirable. Moreover, it soon became apparent that the system as a whole cannot be trusted to count and tabulate all the votes in an equal manner. The 2000 election revealed that the system was procedurally and systemically unsound and in need of drastic, rather than minor, change.

Internet voting has been championed by some as a miracle cure for the current ills of our electoral system. But one must remember that, like any voting system, it too has its potential drawbacks and flaws. After the initial euphoria surrounding the prospects of Internet voting swept the electoral world, the issue was studied in further detail and the promise of Internet voting convenience was replaced by overarching issues of security and reliability. But some in the electoral community have come to realize that, when compared to the current voting technologies, Internet voting is a reasonable voting alternative.

There is no perfect system of voting and there will never be such a system. But the current system is not sustainable and unless the trend of continual electoral failings is reversed, American democracy will continue to suffer. Internet voting may be the only solution to curb dwindling participation rates and add more convenience and stability to the electoral system.

---

161. This system would substantially cut-down the bulk and costs of election materials sent overseas during the election campaign while not radically departing from traditional absentee voting.

162. Ironically, the failing of traditional voting methods in Florida stunted the progress of technological advancement. Instead of moving forward with major initiatives, post-Florida electoral officials are concentrating on fixing the present system before embracing an alternative voting system. Ed Gerck, CEO of Safevote.com, stated, "I would say Internet voting would have been better served without Florida. The same way Florida advanced the need for technology, (was) the same way Florida highlighted the tremendous risks." Farhad Manjoo, *Net Voting? Keep Your Pants On*, <http://www.wired.com/news/politics/0,1283,41648,00.html> (accessed May 9, 2002).

The long-term question then becomes to what level of risk should Internet voting be judged? Should Internet voting be held to the same standard of traditional voting or to a higher standard? Most problems associated with Internet voting are not foreign to the electoral process, just problems cast in a different form. Security and other weaknesses are inherent in the traditional voting methods. So to hold e-voting to a 100 percent secure record would be unfair and create a different playing field.

In the short-term, Internet voting at the polling station could feasibly be instituted within the next few election cycles. The moderate benefits of Internet voting at the polling station, such as less invalid votes and quick, accurate results, come with considerably less risks than remote Internet voting.

Further study into the area is needed to assess the viability and risks of Internet voting.[163] It is imperative that election officials have the foresight and initiative to actively research into this important area of our democracy. Further, and maybe of equal importance, Internet voting can only be implemented when the level of risk associated with its implementation is acceptable to election officials, politicians, and American voters. While it appears that currently Internet voting at the polling station is a reasonable level of risk, the level of risk presently associated with remote Internet voting may simply be too great. Maybe in time, the information garnered from further trials and evolutionary introduction of Internet voting will cause election officials and the voting public to accept remote Internet voting as a safe, effective, and efficient way to vote.

The article will end not with a conclusion but with a question. In response to questioning about Internet voting, Kevin Kennedy, executive director of Wisconsin state election board stated, "(t)here are a lot of questions about Internet voting. For example, how can we be assured that the person who gets a ballot over the Internet is the person who is supposed to be voting and how can we assure the people that there ballots are being properly handled?"[164]

My questions to Mr. Kennedy: First, under the current system of voting in the U.S., how can we be assured that the person who gets a ballot is the person who is supposed to be voting? Second, in light of the problems with the 2000 and 2002 elections, can we really assure the people that their ballots are being properly handled under the current system of voting?

---

163. Because issues relate to security, convenience and cost, the research must be cross-disciplinary and include social scientists, IT specialists, electoral administrators, and lawyers in a collaborative effort.

164. City may conduct elections on Internet. Rinard, *supra* n. 108.

We can only begin to restore our fledgling democracy when we accept that the answers to both questions above are a resounding "no." Once we admit defeat, why not further study Internet voting as a possible remedy for the current state of our democracy?