

Voting in your Underwear: The Promise, Perils and Policy
Implications of Exercising the Franchise on the Internet

© Dana Walker
University of Michigan
Intellectual Property & Information Law
April 2003

© 2003

Dana Walker

For questions or permission requests contact Dana Walker
walkerdm@umich.edu

Elections are one of the most critical functions of democracy. Not only do they provide for the orderly transfer of power, but they also cement citizen's trust and confidence in government when they operate as expected.¹

Voting is one of the most basic political rights provided to citizens in a democracy. Although the right to suffrage is not an absolute, it is regarded as a fundamental privilege under the Constitution.² Our rights and our freedoms derive from the exercise of our franchise. In essence, voting preserves all other rights. Wars have been waged, civil rights movements have been formed, and laws have been enacted in order to expand and guarantee the right to vote. Supreme Court Justice Earl Warren emphasized the importance of voting to democracy by stating, “the right to vote freely for the candidate of one’s choice is of the essence of democratic society, and any restrictions on that right strike at the heart of representative government.”³

In recent years, however, there has been substantial concern about the American voting system. Voter turnout in the U.S. is one of the lowest among all industrial societies, with the Federal Election Commission indicating that 51.3% (105.5 million people) of all eligible voters turned out to vote in the 2000 presidential election.⁴ There is an even more significant problem for 18 to 24 year olds. In 1998, of the 18-24 year old youth voters eligible to vote only 18.5% did so, compared to the 56.5% turnout rate among 45-64 year olds.⁵ This lack of participation is cause for concern. Representational systems gain their legitimacy from the consent of the governed.⁶ Moreover, the 2000 election revealed significant problems unrelated to turnout, including serious flaws in ballot and counting accuracy. These issues, along with broader movements in applying technology to the government sector through e-government, e-democracy or tele-democracy initiatives has led to public and political interest in the promise of using internet technology for voting, otherwise called i-voting.

Proponents hail i-voting as the savior of our democracy – attracting younger voters and enabling the process of voting to be more convenient, more accurate and even more informed. Opponents claim that internet voting will be the downfall of our democratic system – citing problems of security, privacy and unequal access. The purpose of this paper is to look at both the promise and the perils of internet voting in publicly binding elections, positing that considerable legal and policy challenges face i-voting initiatives and arguing that internet voting may be seductive on the surface but could have significant unintended consequences to our current democratic systems.

i-voting: the holy grail of electronic voting

Internet voting is part of a larger movement of electronic or e-voting. However, e-voting and i-voting are not the same. Electronic voting refers to casting a ballot via a broad range of electronic technology, including phones, cable, computers or direct recording electronic (DRE) voting machines. Internet voting, a subtype of e-voting, is specifically defined as casting a secure and secret ballot transmitted via the internet.

Generally, there are three levels of i-voting based on the location where the ballot is cast.⁷ At the first level is *polling site internet voting* where voters would cast their ballot from an existing polling place. In polling site i-voting, election officials would still control the voting platform and physical environment.⁸ At the next level is *kiosk voting* where voting machines would be located in non-traditional polling places like libraries, shopping malls or schools. Here, again the voting equipment would be under the control of election officials. Kiosk voting would expand

the places where voters could cast ballots and voter authentication could be assured if the kiosk was monitored by voting officials.

The holy grail⁹ or “killer app” of all electronic voting initiatives is *remote internet voting*.

Remote voting seeks to maximize voter convenience and access by enabling a voter to cast a ballot from virtually any location that has an internet connection. Although providing the greatest convenience payoff, remote internet voting has substantial security risks because officials would have little control over the voting platform or physical environment.¹⁰

Two large feasibility studies conducted on i-voting¹¹ have suggested that employment of internet voting should progress through these three stages. The Internet Policy Institute study, funded by the National Science Foundation, focused extensively on the technological challenges to internet voting. The report indicated that polling site i-voting offered some benefits and could be “responsibly fielded”¹² within the next several election cycles. The report warned, however, “remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed.”¹³ Nevertheless, many voting pilot programs have skipped the intermediate steps and gone directly to remote i-voting.

why internet voting, why now?

Universities, trade associations, unions and private corporations have deployed i-voting systems in their elections. The National Science Foundation¹⁴, the state of California¹⁵, and several academic institutions have convened large task forces to study the feasibility of voting via the

net.¹⁶ And the allure of i-voting has captured the attention of Microsoft, Unisys, Dell and a number of emerging dot coms.¹⁷

But i-voting is not reserved for private elections, task forces and software developers. The Arizona Democratic Party conducted its 2000 presidential primary via the internet, the first publicly binding internet election in U.S. history.¹⁸ Also in 2000, the Alaskan Republican Party conducted a straw poll over the internet allowing three congressional districts to vote remotely. Four counties in California conducted mock election trials via the internet. And through the Federal Voter Assistance Program, the Department of Defense carried out a small-scale pilot project of remote internet voting for fewer than 100 military personnel stationed overseas.

There are big plans for internet voting: from large states to small towns i-voting is hot. Washington State recently approved a bill to allow online voting for some military and overseas voters in the 2004 election and the pilot project is viewed as the first step toward internet voting for all residents.¹⁹ Local cities, such as Oconomowoc, MN, are also interested in conducting elections via the internet in the very near future.²⁰ And internationally, i-voting is moving ahead with great speed. Italy is testing a large-scale internet voting plan. The Swiss have launched a \$20 million initiative to develop electronic voting systems.²¹ In the UK, 1.5 million voters in 18 local jurisdictions will trial voting on the internet in May 2003, doubling the e-pilot conducted the year previously.²²

enter internet voting: the promise

Imagine your voting experience going something like this. You wake up, pour a cup of coffee and fire up your personal computer. You access the election web site and view a portfolio on those candidates in which you are interested. The candidates' pictures are displayed, and previously recorded statements play through your speakers with startling clarity. The electronic ballot is summoned and you key in your security code. You enter your vote and submit your ballot. Moments later, you are contacted to verify your transmission along with your security code, which is verified at the county clerk's office. Your code agrees and you sign off until this evening, when you will return to instantly view the election results, along with detailed demographic studies and video clips of acceptance speeches.²³

Using the internet to check a bank balance, buy books, find a mate, pay parking tickets, and communicate has become common. Citizens aren't only using the internet for commercial transactions, however, they are increasingly using online channels to communicate with government. A January 2002 survey on the rise of the e-citizen shows that 58% of American internet users (68 million adults) have visited at least one government web site and many have visited more than one. This means that more Americans have visited government web sites than have sought financial information, booked airline flights, or sent instant messages.²⁴

There is also an increasing trend to apply technological solutions to solve two specific voting problems – election administration and voter turnout. The 2000 election focused national attention on administrative problems, including: antiquated equipment; diverse, incompatible, or absent standards on voting recounts; and the inability to get fast and accurate vote counts. As a consequence, Congress has examined an array of reforms including improving polling place access, vote count standardization, ballot design simplification, and the adoption of uniform voting procedures.²⁵

All of these reforms, some would propose, could be helped by technological solutions. Enter the internet. Proponents argue that internet voting would eventually be more cost effective.

Advocates also contend that i-voting would allow for a more accurate and faster vote count.

Some even argue that online balloting would be more accessible to those with disabilities. Most importantly, it is claimed, i-voting would increase voter turnout especially among the most under-represented voting age group in America – 18 to 24 year olds.

The internet does hold some promise in these areas. Voting interfaces could be created that would be more flexible, addressing the needs of a multi-language population. Screens could be customized for people with disabilities. There is also potential for increased accuracy and counting speed. One of the main problems in Florida was the inability of election officials to truly understand “voter intent” and assess over votes (voting for more than one candidate accidentally) and under votes (failing to mark the ballot). Electronic interfaces may be able to assist in this process by making over votes difficult and under votes intentional. In addition, by transferring votes electronically for tabulation, counts could be conducted more quickly, thus avoiding some of the premature vote guesses that plagued the 2000 election.

I-voting advocates indicate that the greatest promise for internet voting is its potential for increasing turnout. They argue that by making voting more convenient people would be more willing to vote. You could literally wake up in the morning, roll out of bed, walk to the computer and cast your ballot in your underwear – forgoing polling place lines, morning commuter traffic or cold weather. Second, i-voting would expand the types of people that vote. Citizens that have generally been under-represented in the election process might be favored in internet voting –

especially youth, overseas military personnel, business travelers, and house-bound voters. According to the Department of Defense, there are approximately 6 million U.S. soldiers and civilians living abroad who have to rely on slow and unreliable mail service to submit absentee ballots.²⁶ And no other group is as disengaged from elections as youth. But internet technology, which has more prevalent usage among the young, may actually encourage this group to vote.

In addition, theoretically, a voter could be more informed – able to check candidate and referendum information via the web and then cast their ballot online. There is some support for this claim, a recent survey on internet usage during the 2002 elections indicated that 57% of those who used the internet for politics went to web sites that provided information about specific issues that interested them and 29% said that the internet was a “very important” source of election information.²⁷

Finally, there seems to be public support for i-voting. A July 2000 survey found that 71% of survey respondents would be “comfortable” using the internet to vote. And a Medill News Service survey found that 41% of Election 2000 nonvoters believe internet voting would improve turnout.²⁸

exit internet voting: the perils

Despite some of its promise, the implementation of a reliable i-voting system poses significant technological and social challenges. Internet voting is more problematic than most electronic commerce or e-government applications because of issues of security, secrecy, and equity.

Technological Hurdles

Technical problems such as computer, server and communication channel security; voter privacy and ballot secrecy; voter authentication; and verifiability and audibility²⁹ pose problems for the full-scale implementation of internet voting systems. While each is an issue on its own, there is substantial balancing between them – it is hard to both increase authentication while at the same time guaranteeing secrecy, for example.

Securing the Communication Channel

Computer-based voting systems are vulnerable to attack at three points – the server, the client and the communication path.³⁰ There is concern in the technical community that large-scale public internet voting elections, because of their high exposure, will be particularly vulnerable to hacking, penetration and denial of service attacks.

Penetration attacks – such as Trojan horse or remote control programs – would allow any group (inside or outside the U.S.) to spy on ballots, intercept and modify votes, or even completely prevent voters from casting a ballot. These attacks are often undetected and could be targeted to specific demographic or geographical groups. There is also the fear that large-scale denial of service attacks³¹ could disenfranchise voters by denying them the opportunity to vote. Finally, there is some chance that spoofing technologies could be employed that would lure voters to connect to imposter sites instead of the legitimate election server. Although there are technologies that can distinguish a legitimate server from an illegitimate one, it is impractical to assume that all voters would have these protections installed on their home computers.³²

Voter Privacy & Ballot Secrecy

In *United States v. Executive Comm. of Democratic Party*, the court concluded that, “secrecy of the ballot is one of the fundamental civil liberties upon which a democracy must rely most heavily in order for it to survive.”³³ Since the adoption of the Australian ballot in the 20th century, Americans have been casting secret votes. There are two essential components to ballot secrecy. First, your vote is private – there is no record of how you voted, there is no way to prove you voted in a specific way, and no one can see your vote. Second, you can tell someone how you voted but you can’t *prove* it. Both facets are essential to guarantee the legitimacy of an election – it helps ensure that voters aren’t coerced while at the same time making it very difficult for citizens to sell their votes.

Remote internet voting poses some serious challenges to the secrecy/privacy part of elections. First, in order for an election to be legitimate only authenticated voters should cast a ballot. However, tighter identification measures weigh against the possibility of true anonymity. PIN numbers, digital signatures or biometric codes provide election officials an electronic trail that links a voter to her vote. Second, secrecy is maintained in a polling place by monitoring the physical environment³⁴. That monitoring is impossible if citizens vote from their home or office. This leads to concerns that work colleagues, system administrators, or internet service providers could intercept or view a ballot. Finally, in remote internet voting it would be relatively easy to show proof of how you voted – the voter could simply take a screen capture of their ballot before submission. Although secrecy and authentication is problematic in the current voting system – especially in absentee ballots – the internet provides an opportunity for fraud on a scale that would be difficult to accomplish in a paper ballot system.

Voter Authentication

Fundamental to the election system is the concept that only authorized voters should be able to vote and that they should only be able to vote once. A voter must be authenticated, but the ballot they cast must be anonymous and the link between the voter and her vote must be irreversibly separated. This is not an issue in e-commerce applications. Though you may send your encrypted credit card via a secure socket over the internet, your name and identifying information is linked to that number. This increases the chance for authenticity but does not ensure anonymity.

Though authentication systems such as smartcards and biometric codes are available, employing those technologies requires a level of technical expertise that certainly is not universal.

Verifiability and Auditability

If the 2000 election proved nothing else it was that an audit trail is necessary. It must be possible to count votes correctly and there must be a way to demonstrate that the election was authentic.

But how and where to store the vote information causes some problems. Ballots cannot be stored on a client computer because it would enable the voter to prove how she voted, thus facilitating the chance of vote selling. If votes are stored on the election server the voter information must be irreversibly detached from the vote.

Interoperability

In reality, a national election is a patchwork of individual state elections each of which is conducted by local officials. Consequently, in order for the election process to operate, the local, county and state election software and computer networks would all have to work together. And

on the client side, an i-voting system must be able to function on a variety of platforms.

However, developing multi-platform compatible software is no easy task. In the 2000 Arizona primary, for example, the voting software did not perform properly on the Macintosh operating system – forcing Mac users to go to a polling place or otherwise be disenfranchised. The need for interoperability has led many to conclude that election software should be open source. Some even argue that an open source model would make the software more secure because the code would be opened up to peer review.

Issues of Access

By far the greatest problem facing internet voting is social, not technological. The right to vote includes the right to participate equally in an election, the right to cast an effective vote, and the right to be free from restrictions that would make voting so difficult or inconvenient that it would equate to disenfranchisement.³⁵ The concern with internet voting is that it would create an inequitable voting system, making voting particularly convenient for a class of citizens who has access to technology while at the same time disadvantaging citizens that don't have that same access.

This “voting technology divide” already exists, where poorer counties throughout the country have less reliable voting equipment. For example, in Election 2000 voters in Florida's Gadsen County, a majority-black area, had a 68 times greater chance of having their votes invalidated than voters in the neighboring majority-white county.³⁶ Gadsen County had outdated and unreliable voting technology, while the adjoining county had state-of-the-art voting machines.

Due to the disparity in internet access, the fear is that i-voting would only make the existing voting technology divide worse. Moreover, given the concomitant technological knowledge that would be necessary in order to run a secure client, some have claimed that remote i-voting represents a new millennium version of a literacy test.³⁷ Not only would a citizen need a computer and an internet connection, but the voter would need a high level of security on that machine. They would need the latest software and hardware installed and would have to ensure all security patches were current. These additional burdens could make any real convenience to remote voting disappear.

legal challenges

The introduction of an i-voting system will require considerable review and reform of federal and state election laws. Issues of jurisdiction, anti-electioneering, liability, and third party software intellectual property protection will need to be examined.

Federalism: Issues of Jurisdiction

Article I §4 of the Constitution grants states broad latitude in the time, place and manner for holding elections for representatives and senators.³⁸ As a result, states can establish and maintain separate and independent election requirements and procedures as long as those requirements do not infringe on a citizen's constitutionally-protected rights. Although Congress generally leaves the administration of the election of its own members up to the states, it may impose additional regulations and penalties for federal elections.³⁹ Control of state and municipal elections, on the other hand, rests entirely with the states.⁴⁰ Each state, therefore, adopts its own electoral requirements and standards and then delegates the actual administration of an election to county officials. Counties then make decisions on what type of voting equipment to buy based on other

priorities within that county. The consequence is a hodgepodge of federal, state and county election laws and practices.

This separation of powers is at the heart of federalism and ensures that states, not the federal government, be responsible for the conduct of federal elections. But state boundaries are difficult to define in the online world and i-voting creates questions about jurisdiction and standardization. As we have seen, internet voting introduces the possibility of automated fraud and attacks that could be executed across state and national boundaries. Acts of abuse committed outside the state or country may not be subject to prosecution under existing state and federal laws. Furthermore, the need for electronic election systems to operate together may lead to more specific federal standards for election equipment, software and even management – driving us closer to a single federal law for election administration.

Anti-Electioneering

The First Amendment protects the right of citizens and the press to freely discuss issues of public concern. The Court has ruled that the government may regulate “the time, place and manner of the expressive activity, so long as such restrictions are content neutral, are narrowly tailored to serve a significant government interest, and leave open ample alternatives for communication.”⁴¹ Today, all 50 states regulate free speech inside and around polling places by limiting electioneering; advocating that the time and place of voting should be separate from campaigning. For example, Louisiana prohibits campaign activity within a 600-foot radius of the polling place, including wearing political buttons and t-shirts.⁴² The Court has consistently

upheld these regulations. In *Burson v. Freeman* the Court affirmed that the state has a compelling interest to protect voters from confusion or undue influence.⁴³

How, then, will states separate voting and campaigning when ballots are cast online? If a voting official cannot control the voting environment it is difficult to control electioneering. Moreover, one of the advantages to internet voting would be the ability for a voter to gather information about a candidate so they could make an informed choice. However, the ability to review candidate information on the same computer screen as their ballot may make it infeasible to enforce electioneering laws. Furthermore, it would be difficult, and certainly not narrowly tailored, to restrict internet campaigning during election times. This concern has led some to advocate that stricter governmental restrictions would need to be placed on candidate sites, especially if those sites were linked to the electronic ballot.

Liability

In the past, election officials have assumed responsibility for voting system problems. But as voting systems increasingly rely on software and network technologies it becomes more difficult for a single election official to be aware of all possible vulnerabilities in the system. This begs the question of who will be responsible if an election goes wrong. If third party software is susceptible because of poor coding, would the software company be liable? If someone voted from work and the network wasn't secure (i.e. didn't have the latest security patches installed) would the workplace administrators be responsible? Or would no entity be accountable for a breakdown.

3rd party proprietary software

An essential element of a secure and fair election is the ability for independent observers to monitor all aspects of the election process. Yet, the reliance on third party propriety software poses problems for voting transparency. Consequently, many are advocating that election software be open and viewable by multiple parties. But proprietary vendors have been less than willing to open up their code for review. Election.com, after the Arizona primary, declined to expose its procedures to scrutiny, arguing that such transparency would compromise its ability to run secure elections in the future.⁴⁴

As private companies become integrally involved in the utmost civic activity – voting – it will be necessary to determine what requirements should be placed on vendors. Laws may need to be enacted that compel vendors to make the details of their system available to election officials, independent observers and the public. Alternately, the government could even create legislation that would force open source software. Or, possibly, a special category of intellectual property law may be necessary to ensure that the software is transparent but at the same time protects the investment of the software creators.

Finally, personal and demographic data is housed in online voting systems, including the storage of digital signatures, PINs, signature images and other personally identifiable information. The collection and storage of this type of data has the potential for abuse. What legal rights will election system vendors have to this data or what laws should be in place to protect the PINs or other authentication codes of citizens who vote via the net.

policy implications

Much has been made about the failures in the American election system – voter turnout continues to drop, ballots are confusing, equipment is antiquated, and vote counting is slow. Many claim the system is in crisis. Considerable pressure has been placed on politicians to reform the ailing structure. Internet voting is only one of such “solutions,” but whether it is the allure of the technology or a real hope it will ameliorate the current woes, it is a solution that has received a great deal of attention. There is political and public pressure to adopt i-voting systems in the near future. However seductive internet voting may be on the surface, there are noteworthy policy questions which need to be answered. Are internet voters different from other voters? Will i-voting advantage one set of ideas over another? What is the acceptable amount of risk we are willing to expose our elections to? What role will (and should) proprietary vendors play in the civic activity of voting? and is the internet the appropriate technology to impose on democratic systems?

The implications of i-voting in equal representation are not trivial. By making voting more convenient for those with ready access, knowledge and comfort of the internet a bias may be created that boosts the potential turnout for a certain class of voters while at the same time diluting the influence of unconnected voters. This voting digital divide not only affects issues of fair representation, but also may advantage certain ideas over others. Will those who have more convenient access bring different values or ideologies? And what effect might that have on current political structures? Some argue that internet voting has the potential to close the civic divide, attracting young voters to the election process. Yet, others worry about weakening the voting power of older populations.

Policymakers will be faced with serious questions about the ramifications of relying on third party private companies to ensure the proper functioning of a democratic system. Election.com's tagline is "Democracy, the upgrade,"⁴⁵ is it appropriate to turn to proprietary companies to upgrade our democracy or is that best left to elected representatives, the public and the legal system? Furthermore, to what extent should vendors be required to make details about their election software available? And how much access and ownership will private companies have over voter data?

Finally, what level of risk are we willing to accept in an online election? Should we require tighter or looser restrictions than a paper ballot system? According to one estimate, 10% of all internet credit card transactions are fraudulent.⁴⁶ A 10% fraud rate in an election would debilitate the country – calling into serious question the legitimacy of the government. And although the internet is fundamentally a distributed system, in order to secure the election process there may be a reaction to close down some aspects of campaign free expression. What do we value more, the free flow of ideas and traffic that characterize the internet or reducing the risk of voter collusion, confusion and fraud?

put your pants back on

The right to suffrage is a fundamental and essential political right. In order for a government to be legitimate the election process must be accurate, secure and representational of all voters. It is in the public's interest to encourage secure voting systems that attract all citizens. However, the right to vote does not include the right to vote in any manner, at any time or in any specific

location.⁴⁷ The state has an interest in protecting the legitimacy and integrity of the election process and as such it was given broad powers to impose voter qualifications and regulate access to the polling place.

I would argue then, that i-voting is not an inevitability, despite what some may predict. Indeed, the current movement toward internet voting smacks of technological determinism. Before we apply technology to a problem we need to figure out what problem we are trying to solve and determine if technology is the appropriate fix. If the problem is that the voting system in the country is unreliable, inaccurate or poorly designed then we should look at solutions that increase reliability, security and usability. The internet does not help this problem, but instead introduces a significant level of risk into the election system. Accuracy and reliability is far more feasible by using current in-person authentication systems combined with reliable voting machines not connected to an insecure communication channel.

If the problem we are trying to solve is low voter turnout then we should seriously consider whether convenience is the main issue keeping voters from the polls. To date, every election reform that has made voting and registration easier (Motor Voter, relaxed absentee ballot requirements, vote by mail, increased polling place hours) has done nothing to increase voter turnout and instead we have seen consistent decreases. Research suggests that information, motivation and person-to-person contact are much more powerful forces shaping voting participation than convenience.⁴⁸

The decision of whether to deploy an internet voting system is political, not technological. Concerns about security, privacy, and authentication are real and pose technological challenges, but the choice to use i-voting is not a technical decision and it is dangerous to view it as such. Technology is not neutral. It brings with it a set of values and those values may be counter-productive to our election systems. Internet technologies are used to create efficiencies and to increase speed. This begs the question as to whether we want to apply speed and efficiency to our election process and our democratic systems. The Founders purposely created a system of government that was not efficient. An elaborate system of checks and balances and a separation of powers created a structure that slowed down lawmaking and direct democracy.

This is not to say that internet technologies cannot be applied to some democracy-building efforts, but should be applied to the right efforts. These technologies do hold promise – opening up channels for diffused and non-commercial authorship and information distribution, creating new communication outlets, and allowing for a free flow of ideas and information. It is in these areas that the internet can be effectively applied to democracy systems, not in balloting.

The internet cannot revolutionize democracy, nor can it revolutionize our election system. The public must make those revolutionary decisions. Though our tendency may be to apply technical solutions to problems, we should guard against adapting our democracy to the available technologies. The internet certainly has a role in the American political culture, but we will be well-served to remember our view of democracy and then adapt the technology to that view – that is the real upgrade.

¹ Internet Policy Institute. (2001). *Report of the National Workshop on Internet Voting*. Washington, DC, p. 1.

² 25 Am Jur 2d, §103 – Voters

³ *Reynolds v. Sims*, 377 U.S. 533 (1964)

⁴ <http://www.fec.gov/pages/2000turnout/reg&to00.htm>

⁵ <http://www.fec.gov/pages/98demog/98demog.htm>

⁶ “ We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty, and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed. That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness.” The Declaration of Independence (U.S. 1776).

⁷ Internet Policy Institute. (2001).

⁸ The real advantage of poll site voting would be vote count accuracy and voter authentication (authentication would be the same as current voting processes). There would be very little value-added to the voter, however.

⁹ Green, Terence. (December 18, 2000). “Voting in a Virtual World.” *New Statesman*. London. Vol. 13, Issue 636. p. xxix.

¹⁰ Though the social and technical issues of each level share some commonalities, remote internet voting has some unique promise and some unique problems. As a consequence, remote i-voting has received the most attention from policymakers, academics, the popular press and the public.

¹¹ The two large feasibility studies include the Internet Policy Institute Study funded by the National Science Foundation and the State of California’s feasibility study.

¹² Internet Policy Institute. (2001), p. 2.

¹³ Ibid.

¹⁴ Ibid.

¹⁵ California Internet Voting Task Force. (2000). “A Report on the Feasibility of Internet Voting.” (available at http://www.ss.ca.gov/executive/ivote/final_report.pdf).

¹⁶ Most notably are Georgia Tech’s Research Institute and the CalTech/MIT voting project.

¹⁷ Center for the Study of Technology and Society. “Special Focus on Internet Voting.” (available at <http://www.tecsoc.org/govpol/focusnetvote.htm>). (accessed March 23, 2003).

¹⁸ Solop, Frederic. (June 2001). “Digital democracy comes of age: Internet voting and the 2000 Arizona democratic primary election.” *PS, Political Science & Politics*, Washington; Vol. 34, Issue 2; pg. 289 – 293.

¹⁹ Sahlberg, Beth. (March 19, 2003). “Online voting deserves overwhelming yes vote.” *Lewiston Morning Tribune*. Idaho. p. 10A.

²⁰ Rinard, Amy. (March 4, 2003). “City may conduct elections on Internet.” *Milwaukee Journal-Sentinel*. p. 03B.

²¹ Diop, Julie Claire. (2002). "Venturing to Vote Online: European Governments Experiment with Internet Elections." *Technology Review*. Cambridge. Vol. 105, Issue 9. pp. 26-27.

²² Office of the Deputy Prime Minister. (January 23, 2003). "E-voting to Face its Biggest Test Yet in May."

²³ Stone, Pamela. (1998). *Electronic Ballot Boxes: Legal Obstacles to Voting Over the Internet*. 29 McGeorge L. Rev. 953.

²⁴ Pew Internet & American Life Project. (2002). "The rise of the e-citizen: How people use government agencies' web sites." (available at http://www.pewinternet.org/reports/pdfs/PIP_Govt_Website_Rpt.pdf).

²⁵ Brien, Peter. (2002). *Voter Pamphlets: The Next Best Step in Election Reform*. 28 J. Legis. 87.

²⁶ "Pentagon's online voting project netted 84 ballots for dtrs 6.2 million." (August 10, 2001). *Associated Press Worldstream*.

²⁷ Pew Internet & American Life Project. (2003). "Untuned Keyboards: Online campaigners, citizens, and portals in the 2002 elections." (available at http://www.pewinternet.org/reports/pdfs/PIP_IPDI_Politics_Report.pdf).

²⁸ Solop (June 2001)

²⁹ According to the National Panel on Internet Voting, voting systems should address the following:

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

³⁰ Internet Policy Institute. (2001)

³¹ In denial of service attacks multiple computers flood the target machine with more requests than it can handle, basically interrupting the communication and disabling the machine.

³² Internet Policy Institute. (2001).

³³ 254 F. Supp. 543, 546 (N. & S.D. Ala. 1966).

³⁴ Of course, voter intimidation and fraud does can occur in a paper ballot system, especially in absentee balloting.

³⁵ 25 Am Jur 2d, General §103

³⁶ Schwartz, Paul. (2002). *Voting Technology and Democracy*. 77 N.Y.U.L Rev. 625.

³⁷ Phillips, Deborah. (January 2001). "Gauging the risks of Internet elections." *Association for Computing Machinery. Communications of the ACM*. New York. Vol. 44, Issue 1; pp. 73-85.

³⁸ U.S. Constitution Art I § 4, “The times, places and manner of holding elections for Senators and Representatives, shall be prescribed in each state by the legislature thereof; but the Congress may at any time by law make or alter such regulations, except as to the places of choosing Senators.”

³⁹ 25 Am Jur 2d, Elections §4

⁴⁰ *ibid*, Elections to state or local office §6

⁴¹ *Burson v. Freeman*, 504 U.S. at 191, 197

⁴² Stone, Pamela. (1998).

⁴³ *Burson v. Freeman*, 504 U.S. at 199, 211

⁴⁴ Gibson, Rachael. (Winter 2001/2002). “Elections online: Assessing Internet voting in light of the Arizona democratic primary.” *Political Science Quarterly*, New York. Vol. 116, Issue 4; pp. 561-583.

⁴⁵ <http://www.election.com>

⁴⁶ Coleman, Kevin. (November 7, 2001). Internet Voting: Issues and Legislation. *Congressional Research Service Report for Congress*. Washington, DC.

⁴⁷ *Burdick v. Takushi*, 504 U.S. 428, 119

⁴⁸ Internet Policy Institute. (2001) and <http://gotv.yale.edu>

Bibliography

Alvarez, Michael & Jonathan Nagler. (2001). *The Likely Consequences of Internet Voting for Political Participation*. 34 Loy. L.A. L. Rev. 1115.

Brien, Peter. (2002). *Voter Pamphlets: The Next Best Step in Election Reform*. 28 J. Legis. 87.

Buchstein, Hubertus. (November 2002). "Cellular Democracy? Internet Voting and Normative Democratic Theory." (available at http://www.newschool.edu/gf/polsci/papers/Buchstein_paper.pdf). (accessed March 16, 2003).

California Internet Voting Task Force. (2000). "A Report on the Feasibility of Internet Voting." (available at http://www.ss.ca.gov/executive/ivote/final_report.pdf).

Carmichael, Christopher. (2002). *Proposals for Reforming the American Electoral System After the 2000 Presidential Election: Universal Voter Registration, Mandatory Voting, and Negative Balloting*. 23 Hamline J. Pub. L. & Pol'y. 255.

Center for the Study of Technology and Society. "Special Focus on Internet Voting." (available at <http://www.tecsoc.org/govpol/focusnetvote.htm>). (accessed March 23, 2003).

Chander, Anupam. (Summer 2002). *Management and Control of the Modern Business Corporation: Whose Republic?* 69 U. Chi. L. Rev. 1479.

Coleman, Kevin. (November 7, 2001). Internet Voting: Issues and Legislation. *Congressional Research Service Report for Congress*. Washington, DC.

Diop, Julie Claire. (2002). "Venturing to Vote Online: European Governments Experiment with Internet Elections." *Technology Review*. Cambridge. Vol. 105, Issue 9. pp. 26-27.

Earle, Thomas & Kristi Bushner. (Spring 2002). *Symposium Constructive Disenfranchisement: The Problems of Access & Ambiguity Facing the American Voter*. 11 Temp. Pol. & Civ Rts. L. Rev. 327.

Elections Canada. (1998). *Technology and the Voting Process*.

Elliott, David. "Examining Internet Voting in Washington." (available at <http://www.electioncenter.org/voting/InetVotingWhitePaper.html>). (accessed March 23, 2003).

Gerck, Ed. (November 2000). "Internet Voting Requirements." *The Bell*, Vol. 1 No. 7, p. 3. (available at <http://www.thebell.net/papers/vote-req.pdf>).

Gibson, Rachael. (Winter 2001/2002). "Elections online: Assessing Internet voting in light of the Arizona democratic primary." *Political Science Quarterly*, New York. Vol. 116, Issue 4; pp. 561-583.

Green, Terence. (December 18, 2000). "Voting in a Virtual World." *New Statesman*. London. Vol. 13, Issue 636. p. xxix.

Harwood, John. (December 22, 2000). "Broken Ballot -- America's Dysfunctional Voting System --- Electoral Choices -- Fixing the System: Lessons From States Hold Hope for Reform - -- Better Technology Is a Key, As Is Educating Voters; But Who Pays the Tab? --- The Pentagon" *Wall Street Journal*. New York. p. A.1

Herrnson, Paul. (2002). *Improving Election Technology and Administration: Toward a Larger Federal Role in Elections?* 13 Stan. L. & Pol'y Rev 147.

Hunter, Garry. (2001). "The Role of Technology in the Exercise of Voting Rights." *Law Technology*, Washington. Vol. 34. Issue 4. pp 1 –14.

Internet Policy Institute. (2001). *Report of the National Workshop on Internet Voting*. Washington, DC.

Jones, Douglas W. (2000). "E-voting: Prospects and Problems." Talk presented at Tau Beta Pi's 31st Annual Symposium. (available at <http://www.cs.uiowa.edu/~jones/voting/taubate.html>). (accessed March 29, 2003).

Larson, Kristen. (2001). *Electronic Commerce in the 21st Century: Article Cast Your Ballot.com: Fulfill Your Civic Duty Over the Internet*. 27 Wm. Mitchell L. Rev. 1797.

League of Women Voters. "Focus on the Voter: Election Reform Symposia Series." (available at http://www.lww.org/join/election/events/fotv_1_remarks1.html). (accessed March 26, 2003).

Morse, Rob. (2002). "E-voting and Democracy: Past, present and future is e-voting a possibility?" *Law Technology*. Washington, Vol. 35, Issue 3; pg. 1 – 31.

McCullough, Theodore. (2002). *Understanding The Impact Of The Digital Millennium Copyright Act On The Open Source Model Of Software Development*. 6 Marq. Intell. Prop. L. Rev. 91.

Noveck, Beth Simone. (Winter 2003). *Designing Deliberative Democracy in Cyberspace: The Role of the Cyber-Lawyer*. 9 B.U. J. Sci. & Tech. L. 1.

Office of the Deputy Prime Minister. (January 23, 2003). "E-voting to Face its Biggest Test Yet in May."

“Pentagon's online voting project netted 84 ballots for dlrs 6.2 million.” (August 10, 2001). *Associated Press Worldstream*.

Pew Internet & American Life Project. (2003). “Untuned Keyboards: Online campaigners, citizens, and portals in the 2002 elections.” (available at http://www.pewinternet.org/reports/pdfs/PIP_IPDI_Politics_Report.pdf).

Pew Internet & American Life Project. (2002). “The rise of the e-citizen: How people use government agencies’ web sites.” (available at http://www.pewinternet.org/reports/pdfs/PIP_Govt_Website_Rpt.pdf).

Phillips, Deborah. (January 2001). “Gauging the risks of Internet elections.” *Association for Computing Machinery. Communications of the ACM*. New York. Vol. 44, Issue 1; pp. 73-85.

Phillips, Deborah. (June 26, 2000). “Is Internet Voting Fair?” *Network World*. (available at <http://www.nwfusion.com/columnists/2000/0626faceno.html>). (accessed March 26, 2003).

Rinard, Amy. (March 4, 2003). “City may conduct elections on Internet.” *Milwaukee Journal-Sentinel*. p. 03B.

République et Canton De Genève. (January 2003). “The Geneva Internet voting system.” (available at http://www.geneve.ch/chancellerie/E-Government/doc/pre_projet_eVoting_eng.pdf) (accessed March 19, 2003).

Rubin, Aviel. (December 2002). “Security considerations for remote electronic voting.” *Association for Computing Machinery. Communications of the ACM*. New York, Vol. 45, Issue 12; pg. 39.

Sahlberg, Beth. (March 19, 2003). “Online voting deserves overwhelming yes vote.” *Lewiston Morning Tribune*. Idaho. p. 10A.

Schwartz, Paul. (2002). *Voting Technology and Democracy*. 77 N.Y.U.L Rev. 625.

Solop, Frederic. (June 2001). “Digital democracy comes of age: Internet voting and the 2000 Arizona democratic primary election.” *PS, Political Science & Politics*, Washington; Vol. 34, Issue 2; pg. 289 – 293.

Stone, Pamela. (1998). *Electronic Ballot Boxes: Legal Obstacles to Voting Over the Internet*. 29 McGeorge L. Rev. 953.

“The Future of Internet Voting.” Transcript from a Symposium Co-Sponsored by The Brookings Institution and Cisco Systems, Inc. (available at <http://www.brookings.org/comm/transcripts/20000120.htm>). (accessed March 29, 2003).

U.S. Government. *Official Website of the President's E-Government Initiatives*. (available at <http://www.whitehouse.gov/omb/egov/index.html>). (accessed April 11, 2003).

Watson, Richard. (January 2001). "A strategic perspective of electronic democracy." *Association for Computing Machinery. Communications of the ACM*. New York. Vol. 44, Issue 1; pp. 27 – 30.

Weisberg, Jacob. (October 28, 1999). "Will Internet voting be good news for American democracy?" *CNN.com*. (available at <http://www.cnn.com/TECH/computing/9910/28/net.voting.pros.cons.idg>). (accessed March 23, 2003).