William & Mary Bill of Rights Journal

Volume 19 (2010-2011)
Issue 4

Article 4

May 2011

Internet Voting, Security, and Privacy

Jeremy Epstein

INTERNET VOTING, SECURITY, AND PRIVACY

Jeremy Epstein*

> Pajama voting may be convenient. It just can't ensure your vote will count.
>
> —Mitch Trachtenberg[1]

> We don't have the technology yet to do [Internet voting] in a secure way, and we may not for a decade or more.
>
> —Ron Rivest[2]

> A government election is something that you don't want to do over the Internet.
>
> —Ben Adida[3]

> [T]he impetus to remove voting roadblocks is, we fear, causing some states to rush recklessly toward Internet voting despite the limits of today's security technology.[4]

ABSTRACT

Internet voting is an appealing concept to most voters, primarily for reasons of convenience ("why can't I vote in my pajamas at a convenient time"), while appealing because of the attractiveness of technology. However, Internet voting is fundamentally different from other types of online transactions such as banking or shopping. In this Article, I describe different types of Internet voting, the advantages and disadvantages from a security and privacy perspective, and provide perspective on the history and evolution of the field.

---

* SRI International. William & Mary Bill of Rights Journal Symposium: Privacy, Democracy, and Elections, October 22, 2010. This article was prepared with support from ACCURATE: A Center for Correct, Usable, Reliable, Auditable and Transparent Elections, under National Science Foundation Grant No. 0524111.

[1] E-mail from Mitch Trachtenberg, Software Developer, to author (Oct. 11, 2010, 11:06 EST) (on file with author).

[2] Alex Altman, *Will Online Voting Turn Into an Election Day Debacle?*, TIME, Oct. 15, 2010, *available at* http://www.time.com/time/politics/article/0,8599,2025696,00.html (quoting Ron Rivest, computer scientist and cryptography expert).

[3] Dan Morrell, *Secret Ballots, Verifiable Votes*, HARV. MAG., May–June 2010, at 10 (quoting Ben Adida, inventor of Helios, an Internet voting system).

[4] Editorial, *Hacked!*, WASH. POST, Oct. 19, 2010, at A14.

INTRODUCTION

Internet voting is so "obviously" good that the move in that direction frequently happens without consideration of the security and privacy issues. The presumption is that increased convenience of voting will increase turnout, especially among younger voters who are more comfortable with technology.[5] Additionally, Internet voting is claimed to offer opportunities for improved voter turnout for overseas and military voters[6] whose rights are protected under the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA).[7] Towards this end, the Military and Overseas Voter Empowerment Act (MOVE) requires that localities make blank ballots available via the Internet and requires forty-five days between when blank ballots become available and the deadline for receipt of marked ballots.[8] Some localities have interpreted these two requirements as requiring localities to offer return of marked ballots over the Internet, although the law does not appear to have that requirement.[9]

In the November 2010 Congressional Election, thirty-three states allowed return of marked ballots over the Internet.[10] Lost in this wholesale move is informed consideration of whether such returns are secure or private. In this Article, I explore the different types of Internet voting, and security and privacy issues associated with different approaches.

Part I reviews the types of activities under the rubric of Internet voting, and the types of voting systems that follow. Part II reviews the advantages and disadvantages of Internet voting, identifying which of the types of voting systems they apply to. Part III discusses some mitigating and aggravating factors. Part IV covers some differences between private and public elections. Part V concludes the paper.

I. WHAT IS INTERNET VOTING?

The term "Internet voting" is used to cover a wide range of technologies. For purposes of this Article, I exclude such activities as voter registration, checking on the status of submitted ballots, and obtaining information about races from official or campaign websites. Rather, I consider "Internet voting" to refer to actions that are used by voters to obtain and potentially return marked ballots using the Internet.

---

[5] *See* Renee Cross, *Internet Voting: Casting Your Vote by Mouse*, LEAGUE OF WOMEN VOTERS OF TEX. EDUC. FUND 3 (2009), http://www.lwvtexas.org/VotingProcedures/Voting%20Proc.%20F&I-%20Internet%20Voting%20final.pdf.

[6] *See* Editorial, *Hacked!*, *supra* note 4; Thad E. Hall, *UOCAVA: A State of Research* (CALTECH/MIT Voting Tech. Project, Working Paper No. 69, Sept. 15, 2008), http://www.pewcenteronthestates.org/uploadedFiles/UOCAVA_Hall_Report.pdf.

[7] 42 U.S.C. §§ 1973ff to 1973ff-6 (2006).

[8] Pub. L. No. 111-84, 123 Stat. 2190, 2321–22 (2009) (passed as part of the National Defense Authorization Act for the 2010 Fiscal Year).

[9] *See id*.

[10] Altman, *supra* note 2.

In this Part, I outline three major independent factors within Internet voting technologies:[11] whether the system is used for blank ballots or ballot return, whether the system is dedicated or non-dedicated for voting, and whether the system is supervised by an election officer. There are many other factors which affect the security of Internet voting, including:

- The types of security analysis performed of the system, including software and hardware, who performs the analysis, and whether the analysis is public.
- Whether the system uses proprietary or open source software.
- The protections in the system against insider threat.[12]
- The managers of the servers used for Internet voting.[13]

As these apply to all types of Internet voting, I do not further divide the universe based on these questions, although the risk from each will differ depending on the three major factors.

The term "Internet voting" is used to refer both to the distribution of blank ballots (printed) to voters via the Internet, through a website or via e-mail, and to the return of marked ballots via the Internet, through a website, e-mail, or fax.[14] For clarity,

---

[11] Other factors are also possible. In a presentation entitled "Thoughts on UOCAVA Voting," before the Election Assistance Commission, the Federal Voting Assistance Program, and the National Institute of Standards and Technology's UOCAVA workshop on August 6, 2010, Professor Ronald Rivest identified six factors—(1) how the ballots are sent to the voter, (2) whether ballots are paper, electronic, or both, (3) whether voters are supervised or unsupervised, (4) whether ballots are marked by the voter (using a pen), a kiosk, or the voter's personal computer, (5) whether ballots are returned by mail, Internet, or both, and (6) whether there is no auditing, moderate auditing, or comprehensive auditing. Ronald L. Rivest, Viterbi Professor of Computer Sci., Thoughts on UOCAVA Voting, Presentation at the Workshop on UOCAVA Remote Voting Systems 4 (Aug. 6, 2010), http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/RIVEST_2010-08-05-uocava.pdf.

[12] Insiders in a voting system can include the vendor of the hardware and/or software, the election officials, poll-workers, maintenance technicians, and others. It is impossible to completely prevent insider attacks, but systems have different levels of resistance to such attacks. *See, e.g.*, DAVID JEFFERSON ET AL., A SECURITY ANALYSIS OF THE SECURE ELECTRONIC REGISTRATION AND VOTING EXPERIMENT (SERVE) 13, 28–29 (2004), http://www.servesecurityreport.org/paper.pdf. The United States Department of Defense's Federal Voting Assistance Program assembled a team of experts, the Security Peer Review Group, to complete the report. *Id.* at 4.

[13] For example, are the servers managed by the local or state board of elections, by a government entity's information technology organization, or by a private vendor?

[14] Although a fax is frequently thought of as being unrelated to the Internet, a large fraction of faxes traverse the Internet by being sent directly from a computer and/or being received by a computer in the form of an e-mail, using services such as eFax. *See* EFAX, http://www.efax.com (last visited April 10, 2011). Neither the sender nor the receiver of a fax can tell if the counterparty used the Internet to send or receive the fax. KENNETH R. MCCONNELL ET AL., FAX: FACSIMILE TECHNOLOGY AND SYSTEMS 173–82 (3d ed. 1999) (comparing standard fax

this Article refers to the former as *blank ballot distribution* and to the latter as *ballot return*. In cases of blank ballot distribution, some other non-Internet mechanism must be used for marked ballot return (e.g., the United States Postal Service or FedEx).

Orthogonally from the question of blank versus voted ballots, the type of system used to cast the ballot is a key differentiator. Specifically, the voter can use a dedicated computer to receive a blank ballot (and perhaps also to return a marked ballot), or the voter can use her personal computer (e.g., laptop, desktop, handheld) to receive the blank ballot (and perhaps also to return a marked ballot).[15] The former is referred to as *kiosk* or *dedicated* voting, while the latter is referred to as *vote from home* or *non-dedicated*.[16] In between variations are also possible, such as using a general-purpose computer in a library, which I group with other non-dedicated methods.

A third orthogonal variation is whether the system used by the voter is supervised by an election official who can check voter identification and provide technical assistance (referred to as *supervised*) or if the system does not have an election official (referred to as *unsupervised*).[17] Supervised systems may rely on the election official or computerized systems to validate the voter's identity, or even a combination, while unsupervised systems must rely on computerized systems to verify identity.[18]

Most combinations of the above three factors are not only possible, but all have unique advantages (and disadvantages). I roughly order these combinations from the least risky to the most risky:

1. Blank Ballot Distribution, Dedicated System, Supervised: A trained election official provides access to a dedicated system that allows a voter to obtain a blank printed ballot. This is conceptually similar to obtaining a blank ballot by mail. The job of the election official is primarily to ensure that the voter gets the correct blank ballot for her. Depending on the system architecture, the election official may also be responsible for protecting the dedicated system against tampering. The election official may

---

technology to PC-fax technology). Therefore, all faxes should be assumed, unless otherwise validated, to use the Internet.

[15] A dedicated computer is one that is not used for other purposes, such as web surfing or e-mail, and is controlled to prevent the introduction of unauthorized software. *See* Jeremy Epstein, *Internet Voting: Will We Cast Our Next Votes Online?*, REVIEWS.COM (Dec. 21, 2009), http://www.reviews.com/hottopic/hottopic_essay_10.cfm (discussing computers dedicated to voting).

[16] *Id.*

[17] Andreu Riera et al., *Internet Voting: Embracing Technology in Electoral Processes, in* ELECTRONIC GOVERNMENT: DESIGN, APPLICATIONS AND MANAGEMENT 80 (Åke Grönlund ed., 2002).

[18] Riera, *supra* note 17, at 80. In states where voter identification is not required, the election official may obtain an affidavit or other validation from the voter. *See, e.g.*, Help America Vote Act of 2002, 42 U.S.C. § 15482 (2006) (explaining that voters can cast provisional ballots by signing affidavits); *Voter Identification Requirements*, NAT'L CONF. OF ST. LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=16602 (last visited April 10, 2011) (providing links to voter identification requirements by state).

also verify identity, but because only blank ballots are provided, this is not critical, as final authorization is typically determined when the ballots are received by the election office based on a "wet signature" (i.e., an ink signature on paper, not an electronic signature).

2. Blank Ballot Distribution, Dedicated System, Unsupervised: A voter may access a kiosk or other dedicated computer to print a blank ballot, but without any assistance or verification from an election official. Because the system is unsupervised, it must be self-protecting against tampering, and must be usable by a voter without training. The lack of an election official may mean that the voting system must verify identity, but because only blank ballots are produced, this is not necessary in most cases.
3. Blank Ballot Distribution, Non-Dedicated System, Supervised: A trained election official provides access to the system. However, because it is not dedicated, mechanisms must be in place to ensure that the ballots produced are correct, even under the assumption that the system has been tampered with (e.g., by installing malicious software).
4. Blank Ballot Distribution, Non-Dedicated System, Unsupervised: The voter must have some mechanism to ensure that the ballot she receives is correct, even under the assumption that the system has been tampered with.
5. Ballot Return, Dedicated System, Supervised: A trained election official provides access to a dedicated kiosk system that the voter can use to obtain, mark, and electronically return a marked ballot. This could include either direct marking (e.g., by filling out a portable document format (PDF) form or a webpage), or indirect marking by printing a ballot and then scanning and returning it via e-mail or a webpage. The job of the election official is to ensure that the voter gets the correct ballot, as well as to protect against potential tampering. The election official may also be responsible for validating the voter's identity; however, this can be done by the voting system (e.g., using a password provided to the voter through postal mail).
6. Ballot Return, Dedicated System, Unsupervised: A voter accesses a kiosk to obtain, mark, and electronically return a marked ballot. As with the blank ballot analogue, the system must be self-protected against tampering, and must be usable by a voter without training. The lack of an election official means that the voting system must verify identity without benefit of access to physical forms of identification (e.g., a driver's license).[19]

---

[19] A voting system could be set up to read driver's licenses or passports. However, without some other mechanism (e.g., automated facial recognition, a closed-circuit camera on the voting machine viewable by an election official, or confirmation with a biometric such as a live fingerprint), there is no proof that the identification provided matches the person using the machine.

7. Ballot Return, Non-Dedicated System, Supervised: A trained election official provides access to the system. However, because it is not dedicated, mechanisms must be in place to ensure that the ballots produced and the marking software are correct, even under the assumption that the system has been tampered with (e.g., by installing malicious software).
8. Ballot Return, Non-Dedicated System, Unsupervised: The voter must have some mechanism to ensure that the ballot she receives and the marking software are correct, even under the assumption that the system has been tampered with.

Any of the blank ballot methods (1, 2, 3, and 4) may provide a method for marking the ballot before printing (e.g., by selecting candidates on an image of the ballot), but not for submitting the marked ballot.

Through the remainder of this Article, I will refer to the above methods either by name or by number.

Each of the above methods can be implemented in many different ways. As examples, the following subsections summarize the architectures of several systems used in Internet voting pilots.

A. District of Columbia Overseas Digital Vote by Mail (DVM)

The District of Columbia DVM system is a ballot return, non-dedicated, unsupervised Internet voting system (method 8) intended for use by UOCAVA voters.[20] It was proposed for use in the November 2010 election, although due to problems identified during the open testing period in October 2010, use of the system for the 2010 election is being limited to blank ballot distribution, non-dedicated, unsupervised (method 4).[21]

In the system as designed, a voter receives a voter identification number and personal identification number (equivalent to a username and password) through the postal mail.[22] She then uses a personal computer to enter her name and PIN.[23] Assuming the voter name and PIN are a correct match and have not already been used in this election, she receives an affidavit asking her to affirm that she is the voter, after which she downloads the correct blank ballot as a PDF.[24] She then uses the PDF reader's capabilities to mark the ballot by checking boxes and/or by typing names for write-in

---

[20] Mike DeBonis, *Hacker Infiltration Ends D.C. Online Voting Trial*, WASH. POST, Oct. 4, 2010, http://voices.washingtonpost.com/debonis/2010/10/hacker_infiltration_ends_dc_on.html.

[21] *Id.*

[22] PAUL STENBJORN, D.C. BD. OF ELECTIONS & ETHICS, D.C. OVERSEAS DIGITAL VOTE BY MAIL SERVICE: AN OVERVIEW & DESIGN MEMO 2 (2010), *available at* http://www.dcboee.us/dvm/DCdvBM-DesignRationale-v3.pdf.

[23] *Id.* at 24. There is no fundamental reason why a handheld device (e.g., the telephone) could not be used, but these were not included in the pilot program.

[24] *Id.* at 8.

candidates, and saves the ballot to her disk.[25] She then uploads the marked ballot to the DVM server, where it is encrypted.[26] The DVM server also stores the voter's affidavit information in unencrypted form.[27] After the election is over, the affidavits and encrypted ballots are copied to an offline server, where the affidavits are reviewed individually by election officials.[28] For those that meet legal requirements, the ballot is decrypted and printed, after which it is treated the same as an absentee ballot.[29]

Although the DVM system was scaled back prior to the November 2010 election,[30] references in the remainder of this paper to DVM are to the system as originally designed (i.e., ballot return).

B. Operation BRAVO (Bring Remote Access to Voters Overseas)

The Operation BRAVO pilot program was used in the November 2008 general election to allow military voters from Okaloosa County Florida to cast ballots from certain military bases.[31] It is a ballot return, dedicated, supervised Internet voting system (method 5). Voters use a system managed by election officials in three locations (England, Germany, and Japan) to cast their votes using a laptop.[32] The votes were uploaded to a server managed by the county.[33] In addition, a paper ballot was generated for each vote, and the paper ballots were subsequently transferred to the Okaloosa County Government where they were counted by hand after election results were certified. No report has been published on the results of comparing the paper ballots to the electronic ballots, or any analysis whether there are any successful or unsuccessful attacks on the BRAVO servers.

II. POTENTIAL ADVANTAGES AND DISADVANTAGES

Internet voting has many perceived advantages and disadvantages, which are described in this section.

A. Enfranchisement

One of the motivations of Internet voting is to increase voter participation. Whether that goal is accomplished is unclear:

---

[25] *Id.* The PDF form includes facilities to prevent voters from overvoting, presuming that the PDF processor the voter selects implements those facilities correctly and has not been subverted. There is no validation of undervoting. Critically, the server does not validate either undervoting or overvoting. *Id.* at 4.

[26] *Id.* at 6, 12.

[27] *See id.* at 6.

[28] *Id.* at 13.

[29] *Id.* at 14.

[30] *See* DeBonis, *supra* note 20.

[31] Pilot Projects, OPERATION BRAVO FOUND., http://www.operationbravo.org/pilot_projects.html (last visited April 10, 2011) [hereinafter Operation BRAVO Pilot].

[32] *Id.*

[33] *Id.*

- In the city of Swindon in the United Kingdom, in local elections that allowed Internet voting, turnout was unchanged from comparable elections.[34]
- In Honolulu, Hawaii in local advisory board elections in May 2009, turnout *dropped* by over eighty percent when comparing the election to the prior election in 2007 for the same positions.[35]

Measuring the actual impact is more difficult:

- If an election provides a new means of voting but does not remove any of the old means, then presumably the number of people who vote will at least not diminish because of that new means. This is a strong argument, but it is not quantitative: it says nothing about how much the turnout will increase—it could be negligible, or hugely expensive on a cost-per-vote basis.
- Specific underserved populations of potential voters vote in small numbers today, in part, because the traditional means of voting present too high a barrier to them.[36] UOCAVA voters and students away at school are two obvious candidate populations. But although the barriers at least for UOCAVA voters have been studied,[37] there is of course no empirical study to measure the actual turnout improvement that Internet voting might offer because they have never had it.
- Surveys show that voters say that they would be interested in voting over the Internet due to convenience.[38] However, the studies do not account for whether those same voters are *more* likely to vote if Internet voting is available. Voters who simply switch from in-person or absentee voting to Internet voting would not contribute to an actual increase in turnout.

---

[34] THE ELECTORAL COMM'N (UK), ELECTORAL PILOT SCHEME EVALUATION: SWINDON BOROUGH COUNCIL (2007), *available at* http://www.electoralcommission.org.uk/__data/assets/electoral_commission_pdf_file/0014/13217/Swindonstatutoryevaluationreport_27190-20110__E__N__S__W__.pdf.

[35] Chad Van der Veen, *Aloha to the Future*, GOV'T TECH., Oct. 2009, at 40–41, *available at* http://digitalmag.govtech.com/GT/GT_Mag_Oct09.pdf. No analysis has noted whether there was a comparable level of interest or closeness in races between the two elections.

[36] *See, e.g.*, Miriam Galston, *Civic Renewal and the Regulation of Nonprofits*, 13 CORNELL J.L. & PUB. POL'Y 289, 309 (2004); Patrick J. Troy, *No Place to Call Home: A Current Perspective on the Troubling Disenfranchisement of College Voters*, 22 WASH. U. J.L. & POL'Y 591, 592 (2006).

[37] *See, e.g.*, Hall, *supra* note 6, at 1, 9–11.

[38] Derek Dictson & Dan Ray, *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*, SECUREPOLL (2000), http://e-voto.di.fc.ul.pt/docs/The%20Modern%20Democratic%20Revolution.pdf (last visited April 10, 2011).

> For example, the addition of early voting has not increased overall turnout, according to Florida studies.[39]

Private elections (e.g., shareholder elections and professional association elections) may give an indication of a somewhat more positive result. The Association for Computing Machinery reports that "the turnout for ACM's elections increased from 11.5% to 14.03% and has remained fairly steady" and "the percentage of international ballots also increased."[40]

A primary goal for Internet voting is to increase participation of UOCAVA voters, who have a significantly lower rate of returned ballots than voters in general, or even compared to absentee voters.[41] Military voters often have difficulty obtaining blank ballots because they move from location to location more rapidly than postal mail can reach them, combined with the unreliability of postal mail.[42] Hence, Internet voting provides the opportunity to increase UOCAVA voter participation, because Internet service is more readily available than postal mail in many locations.

However, in the small number of Internet voting pilots in the United States, there is no evidence that turnout has increased compared to traditional methods of casting ballots.[43] Hence, relying on the Internet as a solution to turnout problems should be treated with some care.

B. Over/Undervote Detection

Voters unintentionally skipping contests on a ballot (undervotes) or voting for too many candidates for a contest (overvotes) have been a historic problem.[44] However, not all undervoting is an error—drop-off issue for voting "down ballot" is a well understood phenomenon. Hence, preventing *undervoting* is not the goal, but rather preventing *unintentional* undervoting.[45]

---

[39] FLA. COMM. ON ETHICS & ELECTIONS, THE EFFECT OF EARLY VOTING ON VOTER TURNOUT IN FLORIDA ELECTIONS: 2010 UPDATE, S. INTERIM REP. NO. 2011-110, at 1, 3 (2010), *available at* http://archive.flsenate.gov/data/Publications/2011/Senate/reports/interim_reports/pdf/2011-118ee.pdf.

[40] E-mail from Ass'n for Computing Machinery to author (Oct. 15, 2010, 16:17 EST) (on file with author).The ACM is the "the world's largest educational and scientific computing society." *Association for Computing Machinery Committee On Ethics Elections*, ASS'N FOR COMPUTING MACH., http://www.acm.org (last visited April 10, 2011).

[41] Hall, *supra* note 6, at 13, 15.

[42] *Id.* at 9–10, 26.

[43] *See, e.g.*, Van der Veen, *supra* note 35, at 40–41 (discussing the low participation in Hawaii's 2009 all-digital election).

[44] Akhil Reed Amar, *Bush, Gore, Florida and the Constitution*, 61 FLA. L. REV. 945, 956, 965 (2009) (noting that on paper ballots, using a pen instead of a pencil can be considered an "undervote" while filling in the bubble for a candidate as well as writing in his or her name is an "overvote" and that these issues came up during the Bush vs. Gore election, as well as others).

[45] Providing an explicit "no selection" option is a way to avoid undervotes, but is not generally allowed by state election laws.

Direct Recording Electronic (DRE) voting systems[46] used in precincts usually provide review screens to warn voters of these omissions or errors.[47] Ballot return systems (methods 5, 6, 7, and 8) can provide undervote and overvote detection and provide warning either as part of software running in the voting device, or in the server that receives the ballot, or both.[48] Blank ballot systems (methods 1, 2, 3, and 4) may provide undervote and overvote detection in the ballot printing system, if they provide a method for marking the ballot before printing.[49]

These requirements for coordination among localities have not been resolved in Internet election pilot programs so far, as each pilot program has been run by a single locality.[50]

Operation BRAVO implemented undervote and overvote detection in its system. The District of Columbia DVM project implemented limited overvote prevention through facilities in the PDF reader; but because voters using non-dedicated computers were not required to use a particular PDF reader, this was implemented inconsistently.[51] The District of Columbia DVM does not implement undervote and overvote protection when the ballots are received by the server. Rather, undervote and overvote prevention happens when the ballots are actually counted, at which point the voter has no opportunity to resolve any problems.[52]

C. Cost and Staffing

Local election officials have long faced the burden of hiring and training enough election officials, and the high cost of running elections with very limited budgets. With the average age of an election official reported to be over seventy,[53] and with Election Day frequently requiring a sixteen hour workday (depending on locality) with minimal pay, finding and training enough workers is difficult. Thus, reducing the staffing levels through automation is an attractive option to localities, as is reducing the cost per voter of conducting the election.

However, the cost and staffing profile for running elections over the Internet is dramatically different from a conventional election. In any of the eight methods described above, the bulk of the cost and effort is in developing, maintaining, and

---

[46] DREs are usually, but not always, touchscreen systems. *See* Paul Herrnson, *Paper Trails, Cryptography and Other Approaches to Vote Verification*, 18 ALB. L.J. SCI. & TECH. 657, 657 (2008).

[47] *See id.* at 659.

[48] If, for example, the ballot is encrypted on the voting device before submission, then checking on the server becomes impossible.

[49] *See supra* Part I.

[50] *See supra* Part I.A and I.B for discussions of pilot programs in D.C. and Florida.

[51] STENBJORN, *supra* note 22, at 4.

[52] *Id.* at 20.

[53] Jim Drinkard, *Panel Cites Poll Workers' Age as Problem*, USA TODAY (Aug. 9, 2004, 12:13 AM), http://www.usatoday.com/news/politicselections/nation/2004-08-08-voting-workers_x.htm (citing a U.S. Election Assistance Commission study).

operating the software used for Internet voting.[54] In addition, depending on the method chosen, there may be additional costs:

- Supervised methods (1, 3, 5, and 7) require election officials to manage the voting systems, much as traditional pollworkers.
- Dedicated methods (1, 2, 5, and 6) require voting equipment.
- Blank ballot distribution methods (1, 2, 3, and 4) require election officials to receive the ballots and treat them as ordinary absentee ballots.
- Some types of ballot return methods (5, 6, 7, and 8) may require election officials to adjudicate the ballots using an online system, thus requiring more training than for the adjudication of paper ballots received through the mail. For example, if ballots are received from an unsupervised system (methods 6 and 8), then an election official must validate the attestation before processing the ballot.

Some of these costs may be prorated across localities. For example, each locality will not place its own dedicated computer system at each military base, nor will each locality have its own election officials. Rather, all localities will need to coordinate to provide common ballot formats so a common system can operate correctly for all voters, and shared election officials will provide supervision.

Additionally, the cost of acquiring software for Internet voting can differ based on factors including:

- Whether the software was obtained off-the-shelf or was developed custom for the state or locality.
- Whether off-the-shelf software is available, and if it is open source or proprietary.
- How much customization is required to meet the localities' needs? (For example, to meet any state-specific requirements).
- Has the software already been approved for use in the state and/or locality as required by law, or does this need to be part of the acquisition process?
- Is additional hardware required to operate the voting system?
- How much hardware redundancy is needed to provide the desired level of reliability?
- Is additional network bandwidth required to support Internet voting? (Most likely for small jurisdictions).
- Does the state or locality have existing infrastructure such as data centers with professional staffing capable of installing and operating an online transaction system? (States probably do, because most can handle some motor vehicle and business transactions, but most localities do not have these capabilities).

---

[54] Joshua F. Clowers, *I E-Vote, U I-Vote, Why Can't We All Just Vote?!: A Survey of the Changing Face of the American Election*, 42 GONZ. L. REV. 61, 79–80 (2006).

Regardless of the acquisition cost of the software and hardware, costs for Internet voting also include training staff to operate the system, constant monitoring of the voting system for security and reliability issues, updating the software to resolve problems found in operation, testing, maintaining and upgrading hardware, etc.

In short, Internet voting has real costs, even though the level of staffing may be reduced through fewer polling places or fewer staff at each polling place. Internet voting experiments to date have had very small numbers of voters, and so the cost per voter has been very high.[55] Table 1 gives *approximate* costs per voter for several recent experiments.

Table 1. Sample Costs for Internet Elections.

Election	**Date**	**Total cost**	**Voters**	**$/voter**
Voting Over the Internet	2000	$6.2M[56]	84[57]	$73,800
Swindon (UK) Municipal Election	2007	£1.2M (est.)[58]	7,647[59]	£157
Democrats Abroad Primary (presidential primary)	2008	$40,000[60]	11,162[61]	$3.58
Operation BRAVO (Okaloosa County, FL)	2008	$700,000[62] (approx)	93[63]	$7,000 (approx)
District of Columbia Digital Vote by Mail[64]	2010	$300,000[65]	900 eligible[66] (approx)	$300[67] (approx)

[55] A noted in Table 1, cost per voter has reached as high as $73,800.

[56] FED. VOTING ASSISTANCE PROGRAM, DEP'T OF DEF., VOTING OVER THE INTERNET PILOT PROJECT ASSESSMENT REPORT 1-6 (July 2009), http://www.fvap.gov/resources/media/voi.pdf.

[57] *Id.* at ES-1.

[58] THE ELECTORAL COMM'N (UK), *supra* note 34, at 6.

[59] *Id.* at 28.

[60] Posting of Stanley Grossman, Int'l Treasurer of Democrats Abroad, to Democrats Abroad (March 10, 2008, 11:05 EST) (on file with author). The amount reflects the money paid to Everyone Counts, the vendor. The costs borne by the organization have not been disclosed.

[61] *Global Presidential Primary Results Report*, DEMOCRACTS ABROAD 2–8 (2008), *available at* http://www.democratsabroad.org/sites/default/files/DA%20Global%20Primary%20Results%20FINAL%20REVISED.pdf. The total number of voters was calculated by adding together the number of Internet voters listed for each country on the chart.

[62] E-mail from Pablo Sarrias, VP of Sales and Mktg. for Scytl, to Pat Hollarn, Supervisor of Elections (Oct. 10, 2008) (on file with author and released to the public).

[63] *Id.*

[64] Due to problems with the system described earlier in this paper, the program was only used for ballot distribution, not ballot return.

[65] *See* DeBonis, *supra* note 20. This figure, provided by the District of Columbia Board of Elections and Ethics (BoEE), does not appear to include in-house costs by the BoEE.

[66] *Id.*

[67] The figure assumes that every eligible voter used the system to vote.

Presumably, the cost per vote would decline in subsequent elections for each of these examples, because the cost of developing software, training staff, and similar tasks would be spread over a number of elections. Additionally, because each of these examples (except Democrats Abroad) was a pilot program, the number of voters was deliberately limited. Finally, as the number of localities participating increase, many of the fixed costs of developing software and processes can be prorated across the participating jurisdictions. The wide range of costs indicates, however, that it is far from clear that Internet voting provides cost savings.

Operation BRAVO required *more* staffing than a traditional precinct—with three locations and a total of ninety-three votes cast, there was at least one staff member and several volunteers on average for every thirty-one voters,[68] as compared to ratios of nearly 100:1 or more in a traditional location.[69] District of Columbia DVM minimized field staffing expenses by using non-dedicated, unsupervised systems (election officials must adjudicate ballots after the election).[70]

As with costs, staffing levels would change depending on the overall structure. For example, an Operation BRAVO-like system that was able to handle ballots from all of Florida (instead of one county) might have a field staffing profile more comparable to a traditional precinct.

D. Coordination

Supervised systems (methods 1, 3, 5, and 7) require an election official to participate in some portion of the voting process. As noted above, the number of localities in the United States precludes each jurisdiction (or even each state) from setting up its own voting sites for UOCAVA voters.[71] Thus, consolidation of responsibility is necessary. If the tasks involved in voting supervision include determining voter eligibility (even including eligibility for a provisional ballot), the election official must be able to make decisions for each of the localities that can be serviced through the voting system. Because states have radically different laws (frequently including that an election official be a resident of the state or even locality of the voter),[72] there may be legal impediments to such consolidation.

For dedicated voting systems, localities (or states) must agree on the requirements for the voting equipment.

---

[68] Operation BRAVO Pilot, *supra* note 31. Depending on state law, there may have been more than one election official for each of the three locations.

[69] *See* U.S. ELECTION ASSISTANCE COMM'N, 2008 ELECTION ADMINISTRATION AND VOTING SURVEY 78–79 (2009), *available at* http://www.eac.gov/assets/1/documents/2008 election administration and voting survey EAVS report.pdf.

[70] STENBJORN, *supra* note 22, at 2, 9.

[71] *See supra* Part II.C.

[72] *See, e.g.*, VA. CODE ANN. § 24.2-115 (2006); ARK. STATE BD. OF ELECTION, RULES FOR ELECTION OFFICIALS (POLL WORKERS) TRAINING § 201 (2009), *available at* http://www.state.ar.us/sbec/pdfs/2010/Election_Officials__Poll_Workers__Training.pdf.

Operation BRAVO avoided coordination problems because it was only for voters in a single locality.[73] Unsupervised systems such as District of Columbia DVM do not require such coordination. Finally, we note that almost every week of the year includes an election somewhere in the country, so coordination becomes a year-round activity, not exclusively for bi-annual November federal elections.

E. Software Compatibility

Dedicated voting systems can be specified for hardware compatibility, while non-dedicated voting system must be able to run correctly on a wide variety of voter computer systems. Both options require more development time than traditional paper ballots, which do not require any voter technology.[74]

Although at first blush compatibility appears simple, given the predominance of Microsoft Windows, in reality there are far more variations than that. Not only are a substantial minority of users using Apple Macintosh computers, and a small minority using Linux and other operating systems, but there are also variations within versions of the operating system.[75] Adding to the operating system variety is differences in browsers: while Microsoft's Internet Explorer is used by a majority of computer users,[76] other browsers, including Mozilla Firefox, Google Chrome, Apple Safari, and dozens of less known browsers, are also in common use.[77] However, users of Internet Explorer 6, for example, are missing capabilities present in more modern browsers[78]—and there are millions of computers still using Internet Explorer 6,[79] including many in the military due to slow replacement cycles.

Furthermore, there are differences in related software used in voting software, such as Java and PDF interpreters. The combination of software makes testing difficult, especially because it is critical that every voter's ballot has the correct layout.

Voting system methods requiring a "thick" client (i.e., one that requires installation of software on the voter's computer) are unworkable, both because of the variety of hardware and operating systems in use that would need to be supported, but also

---

[73] Operation BRAVO was a pilot project limited to Okaloosa County, FL. *See* Operation BRAVO Pilot, *supra* note 31.

[74] *See supra* Part I (summarizing a variety of systems and their requirements).

[75] *See, e.g.*, *Operating Systems Version*, MSDN, http://www.msdn.microsoft.com/en-us/library/ms724832(v=vs.85).aspx (last visited April 10, 2011) (listing different versions of Microsoft Windows).

[76] *Popular Web Browsers*, WEB DEVELOPERS NOTES, http://webdevelopersnotes.com/articles/popular-web-browsers.php (last visited April 10, 2011).

[77] *Id.*

[78] Stephen Shankland, *Microsoft Actively Urges IE 6 Users to Upgrade*, CNET NEWS (Nov. 30, 2009, 3:08 PM), http://news.cnet.com/8301-30685_3-10406468-264.html.

[79] Approximately twenty percent of all computers used Internet Explorer 6 as of February 2010. Stephen Shankland, *Tide Turns Against IE 6 as Usage Drops*, CNET NEWS (Feb. 1, 2010, 2:06 PM), http://news.cnet.com/8301-30685_3-20000033-264.html.

because many voters use computers where installing software is prohibited. In particular, many systems used by military voters are "locked down" to prevent installation of software to protect against many forms of malware, so any solution must rely entirely on software already present on the computer.[80] Because the common baseline is a browser and a PDF reader, anything beyond that risks disenfranchising voters.

Operation BRAVO used dedicated systems so compatibility was not a consideration.[81] District of Columbia DVM experienced significant issues with compatibility—some ballots submitted by Apple Safari users were left blank (even if the voter had selected candidates) and no warning was provided.[82]

F. Privacy and Accuracy When Casting Ballots

Four ballot marking systems (methods 5, 6, 7, and 8) rely on the software to mark the ballot before returning. (Even blank ballot systems can use software for marking before the ballot is printed.) The voter must rely on the software to mark the ballot as instructed. Software bugs or malicious software in the voter's computer could modify the candidates selected before the ballot is returned, even if the voter examines the ballot on the computer screen.[83]

Many users rely on their employers' computers for personal activities such as online banking and shopping.[84] Employers can monitor the online activity of their employees not only by monitoring logs, but also by using "key loggers," which record key strokes and other input.[85] Recent court cases have indicated that employers may monitor personal use of employer-owned computers,[86] which could compromise voter privacy if the computer is used for voting.

---

[80] *See, e.g.*, *PC Lockdown Software*, HORIZON DATASYS, http://www.horizondatasys.com/250416.ihtml (last visited April 10, 2011) (advertising lockdown software).

[81] The project set up three remote voting kiosks, each staffed by workers who set up the kiosk equipment and administered the system. *See* Operation BRAVO Pilot, *supra* note 31.

[82] *See* Jaikumar Vijayan, *Security Concerns Prompt D.C. to Suspend Web-Based Overseas Voting*, COMPUTERWORLD (Oct. 6, 2010), http://www.computerworld.com/s/article/print/9189578/_security_concerns_prompt_D.C._to_suspend_web_based_overseas_voting.

[83] The Zeus botnet uses this technique to enable financial fraud, hiding from the user of a banking website transactions that siphoned money from the victim's account. This is known as a "man in the browser" attack, because the money (or votes) are manipulated by the voter's browser (or other voting software). *See* Atif Mushaq, *Man in the Browser: Inside the Zeus Trojan*, THREATPOST (Feb. 19, 2010, 11:35 AM), http://threatpost.com/en_us/blogs/man-browser-inside-zeus-trojan-021910.

[84] J. Beam, *How Do Employers Monitor Internet Usage at Work?*, WISEGEEK, http://www.wisegeek.com/how-do-employers-monitor-internet-usage-at-work?html (last visited April 10, 2011).

[85] For a report of the use of keyloggers to steal financial data see *PC Tools Warns of Emerging, Complex Variant of Keylogger Threat Targeting Banks*, MARKETWIRE (Mar. 10, 2006, 9:00 AM), http://www.marketwire.com/press-release/PC-tools-warns-of-emerging-complex-variant-of-keylogger-threat-targeting-banks-682384.htm.

[86] *See, e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 559–60 (S.D.N.Y. 2008) (noting that courts have "routinely" found that employers may access

G. Privacy of Returned Ballots

Election officials have well-defined practices to ensure that absentee ballots received via postal mail are properly adjudicated without allowing connections between voters and ballots.[87] Blank ballot systems (methods 1, 2, 3, and 4) are equivalent to other absentee ballots, and hence the mechanisms should require minimal changes.

Ballot return systems (methods 5, 6, 7, and 8) are more complex. Supervised systems (methods 5 and 7) may not have any voter-specific information associated with the electronic ballot, if the election supervisor prevents access to the voting system except by authorized voters, although correlations may be possible through records kept by local election supervisors.[88] Unsupervised systems, whether dedicated or not (methods 6 and 8), require that the voter sends some form of identifying information along with her ballot, so that the vote can be adjudicated by the election official upon receipt. This requires careful design so the election official cannot make the adjudication decision based on the voter's ballot, nor can the election official see the voter's ballot associated with her identity even after the adjudication decision is made.

H. Vulnerabilities

Every software system contains vulnerabilities, even when extensive searches are made to identify and fix vulnerabilities.[89] The opportunities for vulnerabilities, and the risks from those vulnerabilities depend on the system architecture.[90] Broadly speaking, vulnerabilities in Internet voting systems can occur in three places: the client (the computer used by the voter for casting the ballot), the network (which transmits the blank and/or marked ballots), and the server (where the blank and/or marked ballots are stored).[91]

---

private files on work computers and that employees do not have a reasonable expectation of privacy on employer-owned computers).

[87] For example, some locations use double envelopes where the outer envelope contains the voter affidavit. Once the affidavit is approved, the ballot in an inner envelope is separated from the outer envelope, and all inner envelopes are mixed before any are opened. *See, e.g.*, VA. CODE ANN. § 24.2-710 (2006). Of course, such schemes are not perfect—for example, when only a small number of ballots in a precinct or ballot style are cast, or when an election official deliberately subverts the system by marking inner envelopes with identifying information.

[88] For example, if the election supervisor keeps a record of who voted at what time or in what order, as is required in some states, that could be correlated with the time of ballot receipt to compromise voter privacy. *See, e.g.*, FLA. STAT. § 101.23 (LexisNexis 2010).

[89] *See* Microsoft, Trustworthy Computing: Software Vulnerability Management at Microsoft 4–5 (July 2010), http://www.microsoft.com/downloads/info.aspx?na=46&SrcFamilyId=3C87D741-8427-456D-9BB3-2BDB2D0272E5&SrcDisplayLang=en&u=http%3a%2f%2fdownload.microsoft.com%2fdownload%2fB%2fB%2f3%2fBB3DA45E-87FD-4398-B85D-21ADF2473D6E%2fSoftware+Vulnerability+Management+at+Microsoft.pdf.

[90] *See id.*

[91] INTERNET POLICY INST., REPORT OF THE NATIONAL WORKSHOP ON INTERNET VOTING:

Classes of client vulnerabilities may include:

- Credential theft.[92] For example, malware[93] that forwards the voter's credentials (e.g., username and password) to someone who can cast the ballot later.
- Modification of the blank ballot presented to the voter.[94] For example, malware in the client could reorder or eliminate candidates or contests from the ballot or change timing marks[95] on the ballot.
- Modification or disclosure of the voter's ballot.[96] For example, sending a duplicate copy of the voter's ballot to another web site where it could be used for coercion without the voter's knowledge.
- Redirection of the voter using phishing. For example, an e-mail to a voter appearing to be from a preferred candidate[97] could give a link to a fake site instead of the real voting site.[98]

Classes of network vulnerabilities may include:

- Domain redirection.[99] This technique exploits the Domain Name System (DNS) so requests for a particular web site are redirected to a fake site.[100]

ISSUES AND RESEARCH AGENDA 13–16 (2001), *available at* http://news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

[92] *See* PHILIPPE BEAUCAMPS ET AL., ON THE USE OF INTERNET VOTING ON COMPROMISED COMPUTERS 2 (2009), *available at* http://www.loria.fr/~beaucphi/articles/beaucamps-reynaud-marion-filiol-internet_voting-iciw09.pdf (defining "malware" as any type of program with unwanted characteristics, such as viruses or spyware).

[93] I assume such malware can be readily installed through techniques such as "drive by downloads" or having voters open attachments that install software. Surveys show that between 10% and 50% of home computers in the United States have one or more types of malware present.

[94] *See* INTERNET POLICY INST., *supra* note 91, at 13 (discussing the three main points of attack).

[95] Timing marks are indicators, usually along the side, that help scanners find the location of the marked region (e.g., the bubble to be colored).

[96] *See* BEAUCAMPS ET AL., *supra* note 92, at 3.

[97] For example, a Democratic candidate sending a link to a fake site to Republican voters or vice versa. This is the high-tech equivalent of fliers used in minority neighborhoods of the form "due to high turnout, Republicans vote on Tuesday and Democrats on Wednesday," thus disenfranchising voters who are unfamiliar with election laws.

[98] *See* U.S. PUB. POLICY COUNCIL OF THE ASSOC. FOR COMPUTING MACH., ISSUE BRIEF: INTERNET VOTING AND UNIFORMED AND OVERSEAS CITIZENS ABSENTEE VOTERS 5 (2010), *available at* http://usacm.acm.org/usacm/PDF/IB_Internet_Voting_UOCAVA.pdf.

[99] *See* INTERNET POLICY INST., *supra* note 91, at 17.

[100] DNS is the equivalent of the "white pages" for a phone system. Giving false DNS addresses is like changing a listing in the phone book to the wrong phone number. *See Definition*

This would be very effective in sending a voter to a fake web site for casting their votes.

- Routing redirection.[101] This technique exploits the Border Gateway Protocol (BGP) so network packets directed to particular IP addresses are redirected to a fake site.[102]
- Network reconfiguration.[103] If network devices such as routers are misconfigured (or have unchanged or weak passwords), voters can be redirected away from the web site.

Classes of server vulnerabilities may include:

- Server break-ins.[104] This broad class of vulnerabilities refers to gaining access through bugs in the operating system and/or applications.

Any of the above types of vulnerabilities have the opportunity to compromise ballot privacy and ballot integrity.

Operation BRAVO, by using a dedicated system, reduced the risks of client-side vulnerabilities, since the potential is present for ensuring that only authorized software is present (ignoring potential malware inserted by insiders). Additionally, by using a Virtual Private Network (VPN) for transmitting data from the voting kiosks to the central server, most network issues can be detected (since the VPN will fail), although they cannot be prevented.[105] The main risk for Operation BRAVO is server vulnerabilities.[106] Although there was no open opportunity for identifying vulnerabilities, a team examined the system and provided a positive report on its strengths.[107]

---

of Domain Name System (DNS), *in* A DICTIONARY OF COMPUTING (John Daintith & Edmund Wright eds., 6th ed. 2008).

[101] *See* Michael Kassner, *BGP: Yet another Internet time bomb*, TECHREPUBLIC (Sept. 14, 2008, 7:41 PM), http://www.techrepublic.com/blog/networking/bgp-yet-another-internet-time-bomb/663.

[102] BGP instructs packets how to get to their destination. Giving false BGP information is like changing the road signs so drivers get lost or go to the wrong address. *See Definition of Border Gateway Protocol*, *in* A DICTIONARY OF COMPUTING, *supra* note 100.

[103] *See* SID STAMM ET AL., DRIVE-BY PHARMING 1, 4 (2006), *available at* http://www.cs.indiana.edu/pub/techreports/TR641.pdf.

[104] *See* INTERNET POLICY INST., *supra* note 91, at 13–14.

[105] *See* Paul Ferguson & Jeff Huston, *What is a VPN?—Part 1*, INTERNET PROTOCOL J. June 1998, at 1, *available at* http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_1-1/ipj_1-1.pdf.

[106] *See* EKR, *DC's Internet Voting Pilot*, EDUCATED GUESSWORK (July 1, 2010, 2:21 PM), http://www.educatedguesswork.org/2010/07/dcs_internet_voting_pilot.html.

[107] Pat Hollarn & Carol Paquette, Operation BRAVO Found., Presentation to the National Association of Secretaries of State Voter Participation Committee, Innovative Approaches to Military Voting: Okaloosa County, Florida Remote Voting Project Overview and Proposed

The District of Columbia DVM, because it uses non-dedicated voting systems, is at risk for all of the client and network vulnerabilities. The District provided an open testing period and open source for public review, which enabled identifying critical server vulnerabilities, as well as critical network misconfigurations.[108]

I. Fraud/Coercion

Any form of unsupervised voting is subject to fraud and coercion. This has historically been true with absentee ballots, including in locations such as nursing homes.[109] There is no reason to believe that Internet voting will be any different—once the voter receives her credentials, those credentials may be sold, or the voter may be coerced to cast her vote in a particular fashion. There are methods possible to allow Internet voting while limiting coercion. For example, in Estonia, voters can cast as many votes as desired, where only the last vote (before the closing time of the election) is counted.[110] Thus, there is no incentive for anyone to buy votes, and coercion is reduced. However, such schemes have not been used in the United States, in part because they require storing information about the voter identity with the votes so they can be replaced, thus increasing the risk that voter privacy will be compromised.[111]

III. AGGRAVATING AND MITIGATING FACTORS

The risks of Internet voting can be aggravated or mitigated based on factors including:

- How small or large is the locality? Large localities will tend to have contests that are higher value, and hence of more interest to an attacker who might seek to influence the results. Additionally, large localities are more likely to have larger and more skilled information technology staffs who are more familiar with the nuances of setting up Internet servers and keeping them securely updated.

Next Step (Feb. 7, 2009), *available at* http://www.operationbravo.org/documents/NASS%20VP%20Briefing.pdf.

[108] *Digital Vote by Mail*, DC BD. OF ELECTIONS & ETHICS, http://www.dcboee.us/DVM/ (last visited April 10, 2011); Jeffery Smith, *Update: District Suspends Digital Vote by Mail Pilot*, CIVSOURCE (Oct. 7, 2010), http://civsourceonline.com/2010/10/07/update-district-suspends-digital-vote-by-mail-pilot.

[109] Jessica A. Fay, *Elderly Electors Go Postal: Ensuring Absentee Ballot Integrity for Older Voters*, 13 ELDER L.J. 453, 454 (2005) (noting that nursing home voting is subject to fraud).

[110] Dan S. Wallach, *Voting System Risk Assessment Via Computational Complexity Analysis*, 17 WM. & MARY BILL RTS. J. 325, 342 (2008) (discussing the Estonian voting system).

[111] *See id.* at 343 (discussing the information stored in computers for the Estonian voting system).

- Who manages the election? Even with traditional elections, many localities rely on private sector providers to set up ballots, program voting machines, diagnose problems, etc.[112] When moving to Internet elections, will the private sector provider set up servers to be used by voters, or will it be done by the local election officials? If by the private sector, what security and privacy policies are enforced by the provider?
- Who provides the software? Is the software used for the Internet election provided by the locality, state government, or private sector? If the software is provided by the private sector, what rights does the government have to access the source code and other information? Does the vendor use open source or proprietary software? Although there is no inherent advantage to either open or closed source, open source can provide greater voter confidence.[113]
- What level of analysis and accreditation? Has the software, regardless of provenance, been subject to analysis by experts in accessibility, usability, privacy, and security? What processes are used for accreditation before putting the software into use?
- Where does the software run? For cost reasons, many services are being shifted into "the cloud."[114] Running election software in the cloud increases the risk from insiders, as the software may be running on computers in foreign countries, as well as on servers not controlled by either the localities or their vendors (who rely on third-party cloud providers).[115]
- How are voters provided credentials to access their ballots? As many voters only cast ballots every two or four years, expecting voters to remember a password is unreasonable, and even expecting them to have the same e-mail address as they used at the last election is unrealistic. Relying on data like Social Security Numbers (SSN) does not work, since many people have access to SSNs,[116] and could cast votes on behalf of the voter. The best solution is to mail out credentials (via the postal service) in advance of the election.

---

[112] *See* Harry Neufeld, *Computerizing Electoral Administration*, *reprinted in* 7 ELECTIONS TODAY (Special Issue) 31, 35 (1998).

[113] James W. Paulson et al., *An Empirical Study of Open Source Software Products*, 30 IEEE TRANSACTIONS ON SOFTWARE ENGINEERING 246 (2004), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1274044&userType=inst (discussing the advantage of open-source software products).

[114] *See* Francoise Gilbert, *Cloud Service Contracts May be Fluffy: Selected Legal Issues to Consider Before Taking Off*, 14 J. INTERNET L. 1 (2008) (stating the cost effectiveness of using cloud computing systems).

[115] David Binning, *Top Five Cloud Computing Security Issues*, COMPUTERWEEKLY (Apr. 24, 2009, 2:46 PM), http://www.computerweekly.com/articles/2010/01/12/235782/top-five-cloud-computing-security-issues.htm.

[116] *Fact Sheet 10: My Social Security Number—How Secure Is It?*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/fs/fs10-ssn.htm (last visited April 10, 2011).

IV. PRIVATE ELECTIONS

A private election is an election held by a private organization, such as an association or corporation to elect members of a board or decide questions.[117] There are fundamental differences between private and public (government) elections,[118] including:

- There may be no right to a secret ballot, or it may be by practice rather than a legal requirement.
- The notion of one person, one vote may not apply. For example, in shareholder elections, votes may be based on the number of shares held, and different classes of shareholders have different votes per share.
- There is no tradition of in-person voting, as there is for public elections. Hence, the cost and staffing comparison should be of mail-in ballots vs. online ballot submission.
- Elections are only open to members (for associations) or stockholders (for corporations), not the general public.
- There is no requirement for certification of the systems used for elections.

In some states, primary elections are private elections run by the State, where the traditional guarantees of ballot secrecy do not apply.[119] However, this Part is focused on non-governmental elections.

The most critical difference between public and private elections, however, is the difference in threat models.

- In corporate elections, it is extremely rare for a board member endorsed by management to lose an election, or for a position opposed by management to win.[120] Similarly, most volunteer organizations (e.g., professional groups) have relatively uncontested elections, so the results are frequently preordained.[121] Hence, determining "abnormal" results is easy, compared to public elections where the "correct" result may be hard to identify.

---

[117] *See* Carol A. Jones, *Time and Method—Election of Directors by Shareholders*, *in* FLETCHER CYCLOPEDIA OF THE LAW OF PRIVATE CORPORATIONS § 288 (William Meade Fletcher ed., 2006) (discussing corporate elections).

[118] Anil Shivdasani & David Yermack, *CEO Involvement in the Selection of New Board Members: An Empirical Analysis*, 54 J. FINANCE 1829, 1829 (1999) (stating differences between private and public elections); Stephen Labaton, *S.E.C. to Propose Change in Election of Boards*, N.Y. TIMES, May 20, 2009, at B3.

[119] *See* J. A. Connelly, Annotation, *Validity and Effect of Statutes Exacting Filing Fees from Candidates for Public Office*, 89 A.L.R.2d FED. 864, 866 (1963) (stating that primary elections can be deemed private affairs).

[120] Shivdasani & Yermack, *supra* note 118, at 1829.

[121] *See* BOARDSOURCE, THE NONPROFIT BOARD ANSWER BOOK: A PRACTICAL GUIDE FOR BOARD MEMBERS AND CHIEF EXECUTIVES 83–84 (Robert C. Andringa ed., 2d ed. 2007) (stating that the preferred way to elect directors for a nonprofit organization is to submit an uncontested list for a vote).

- The value to an adversary in manipulating a private election is generally much lower than manipulating a public election, especially when considering that truly anomalous results can be detected.[122] The publicity value to an attacker of subverting a private election is low, and in many cases (especially for non-profit groups) candidates are only too happy to lose!
- In private elections, voters already have known identifiers (e.g., account or member numbers) that can be used more accurately than quasi-public identifiers like Social Security Numbers.[123]

Hence, the use of Internet voting for private elections may be appropriate, despite the risks associated with public elections. Certain private elections, such as union elections, are closer to public elections, and are probably not suitable for Internet voting.[124]

V. CONCLUSION

Internet voting is widely claimed to improve voter turnout and reduce costs. However, there is no justification for either claim. Additionally, there are significant risks to voter disenfranchisement. Localities considering moving to Internet voting need to consider the technical factors, focusing on key parameters such as blank ballot distribution vs. ballot return, dedicated vs. non-dedicated systems, and supervised vs. unsupervised systems. Blank ballot distribution may be feasible, especially with dedicated systems, but other types of Internet voting are too risky to be used for public elections.

---

[122] Labaton, *supra* note 118, at B3.

[123] AMY L. GOODMAN ET AL., PRACTICAL GUIDE TO SEC PROXY AND COMPENSATION RULES § 15.04 (West ed. 2009) (stating that shareholders are sometimes identified by personal identification numbers known as "PINs").

[124] *See* Clyde W. Summers, *The Privatization of Personal Freedoms and Enrichment of Democracy: Some Lessons from Labor Law*, 1986 U. ILL. L. REV. 689, 712–14 (discussing some similarities between private union elections and public elections).