iVote Advisory Committee

Final Report

August 21, 2015

Utah Lieutenant Governor

Spencer J. Cox

Chair:

Alex Lawrence

Committee Members:

Senator Curt Bramble
Ryan Cowley
Thad Hall, Ph.D.
Ricky Hatch
Julie Knecht
Jennifer Morrell
Sherrie Swensen
Brian Witten
Representative Chavez-Houck
Representative Jon Cox
Jesse Harris
Sara Jones
Mark Mitchell
Sheri Newton
Phil Windley, Ph.D.

Introduction:

The possibility of implementing Internet voting has grown in popularity over the years. Internet voting has inspired numerous studies and pilot projects, and Estonia has even implemented it nationally. The purpose of this report is to study the potential benefits and challenges of implementing Internet voting in Utah. The authors of this report are the members of the iVote Advisory Committee assembled by Lieutenant Governor Spencer J. Cox. Members include state legislators, election officials, and technology and security experts.

As we sought to determine whether conducting an election entirely over the Internet is beneficial, and most importantly, whether it is secure and feasible, we first looked at how Utah currently uses the Internet to help military and overseas voters. We then calculated potential benefits of offering voting entirely on the Internet. Next, we examined potential security weaknesses threatening the stability and accuracy of Internet voting as well as possible mitigation strategies. The final sections discuss potential applications of Internet voting as well as policy implications that must be considered if we adopt Internet voting.

Section 2: Current Practices that Use the Internet

Currently, Utah election officials have the authority to send ballots via the Internet to uniformed members of the military, overseas citizens, and individuals with disabilities. There are two methods by which these voters may receive and transmit a ballot electronically. First, election officials may send the voter a ballot as an attachment to an email. The voter fills out the ballot, scans the ballot into an electronic format, and emails the ballot back to the election official.

The second method allows the voter to use an online ballot marking system. Utah is currently involved with a pilot project funded by the Federal Voting Assistance Program and implemented by the organization Everyone Counts. Everyone Counts' system provides the voter with the ability to electronically mark and send their ballot over the Internet without the need to print and scan their ballot.

Whichever method these voters use to retrieve and transmit their ballots, they must sign a paper affidavit relinquishing their right to a secret ballot. Once the ballot arrives at the election office, whether through an email or through Everyone Counts, election officials duplicate it by hand onto an official paper ballot and scan it into the tabulation system. While this process expedites the transmission of the ballot to and from the voter, this labor intensive process introduces the possibility of human error in the duplication process.

Although these two methods utilize the Internet in some way, neither method can be considered full Internet voting. Voters must still print out the affidavit and send it to the county clerk, and county clerks must duplicate ballots by hand to count them.

Section 3: Potential Benefits of Internet Voting

Giving voters the ability to vote completely over the Internet has several advantages. Making voting more convenient may increase the number of voters participating in elections and engaging in the political process. By allowing individuals to vote from a location of their choosing, they are able to vote without having to compromise their work or child care schedules. It may also improve turnout among younger voters because they may be more likely to respond to Internet voting favorably.

Internet voting may also increase turnout from voters who have disabilities or have challenges leaving their home or living facility. One in seven voters in Utah has accessibility needs, but voters with disabilities vote at a significantly lower rate for several reasons. First, some voters cannot get to the polls because of health reasons or a lack of transportation options. Second, many polling places are not accessible.

Third, using a voting machine can be intimidating and does not provide features some groups need. According to a 2012 national survey, 45% of people with disabilities surveyed reported trouble using the voting machines. Some voters are embarrassed or fear ridicule because of the additional time needed to use the accessible features on the machine while others wait in line.

In some cases, people with disabilities frequently experience awkward delays and may leave without voting. Occasionally, poll workers may not have adequate disability training. They must absorb a tremendous amount of information in only a few hours of training. Therefore, they may lack the understanding of the accessible features of machines, and do not understand how to properly assist people with disabilities at the polls. These issues that voters with disabilities encounter when trying to vote traditionally may be avoided by implementing Internet voting. Citizens with disabilities need not worry about leaving the house or navigating an inaccessible polling place. Internet voting could allow voters with disabilities to vote with the electronic equipment and software programs that meet their specific needs.

Other potential benefits of Internet voting include the reduction of election administration costs by reducing the number of physical voting machines, by-mail ballots, and poll workers needed to conduct an election. Another potential advantage could be the ability to publish election results earlier. However, because the implementation of Internet voting is not widespread, many of these benefits are not yet proven and are susceptible to risk.

Section 4: Risks to Internet Voting

Internet voting possesses several inherent risks, which include legitimacy, accuracy, and ballot privacy. A plausible threat exists for talented and malicious hackers to decide election outcomes by compromising the security of browsers, operating systems, counting, and auditing software. Similarly, the principles of fair elections--particularly the secrecy of an individual's vote -- must remain sacrosanct. This secrecy protects voters from intimidation and protects democracy against vote buying where citizens are

effectively bribed to vote a certain way. Potentially weak election security may also prove to be too much of an attractive target for some nation states, criminal actors, activists, political partisans, and insiders to resist.

The significant challenge to Internet voting is getting a count that is trustworthy and reliable while also continuing to protect the secrecy of the ballot. In short, computer security challenges are the primary problem. Most current computer operating systems, and many standard computing practices, are inherently insecure. Given all of the risks, including malware, computer viruses, and distributed denial of service (DDoS) attacks, it is not possible to ensure that votes are cast and counted properly when voters can use any hardware and operating system of their choosing. Recent news reports about security compromises at Target, UPS, Community Health Systems, Sony, and JP Morgan Chase, to name a few, point out not only the weaknesses in the system and the power of hackers to take advantage of those weaknesses, but also the difficulty for even professional corporate computer security teams to keep malicious hackers at bay despite owning, creating, and operating all of the hardware and software. In that context, the average voter stands little chance of keeping control of their vote unless we narrow the set of hardware and software to a sufficiently secure set of hardware and software for them.

In many cases we are able to avoid the inherent insecurity of the internet because the value received from attacking a weakness is not sufficient to attract the attention of those who exploit these weaknesses for gain. In other cases there is significant value to be gained by attacking a system. Yet despite this, the use of the Internet for commerce, enterprise systems, data dissemination, and other activities continues to grow because the rewards for using the system outweigh the risks and those risks are mitigated by other factors.

Internet voting presents a similarly valuable target for hackers. Elections have consequences, and the ability to influence an election is enticing to those who have a stake in the outcome. The list of potential attackers is large: individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists have a stake in the outcome of elections. We can expect them to use weaknesses in the voting system to gain influence or simply cause mischief.

Some people point out that other activities use the Internet to great benefit, specifically using the refrain, “If we can shop online, why can’t we vote online?”[1] Despite growing security problems, online shopping and other activities continue to grow. However, Internet voting has four properties that set it apart from other online activities like shopping:

1. **Secret ballots are required.** How a specific voter voted is kept secret from election officials and others. This measure protects the validity of the vote by making it more difficult to coerce or pay people to vote a particular way and by ensuring that they will not have to answer to others for their decisions in the polling booth. Internet voting initiatives have to ensure secret ballots.

[1] Jefferson, David. "If I Can Shop and Bank Online, Why Can't I Vote Online?" Verified Voting. November 2, 2011.

2. **Computing environment is uncontrolled.** To be fully open, Internet voting would have to allow people to vote from their own devices in their own homes or businesses to maintain accessibility. But a study in 2010 demonstrated that 48% of 22 million computers were infected with a virus and "over a million and a half [were] infected with crimeware/banker Trojans."[2] Any fully open Internet voting system has to be able to run on a collection of computers that is not only, "not under the control of the voting authorities," but also "not wholly under the control of the voter either."

3. **Major elections are infrequent.** To some degree, security of online commerce has improved dramatically over the years through constant daily refinement of processes built on years of frequent transactions in high volume. This allows the defenders to improve security of e-commerce every day and forces attackers to slowly reveal their strategy with every attack revealed every day. In contrast, major elections are infrequent, giving the attackers years to plan an attack against infrastructure exercised roughly once or twice every year. Despite the far higher volume and frequency of online commercial transactions, online commerce has a residual fraud rate, even after the system has been continually improved over the years. Reports show 32% of Americans have claimed credit card fraud such as fraudulent charges due to identity theft, card theft, or security breach in the past five years.[3] Obviously, it would not be acceptable for 32% of Americans to have their vote tampered with.

4. **The margin for error is very small.** Elections are often decided by very small margins. Unlike a business transaction where the likelihood of fraud can be statistically calculated and then factored into the cost of doing business, there is no margin in a voting scenario to use in mitigating fraud. The margin for fraud has to be very near zero. Moreover, as many people wonder, "if we can do trillions of dollars in e-commerce transactions via the Internet, then why can't we vote via the Internet?" That question fails to recognize that the fraud dispute process for e-commerce transactions, and any credit card transaction, can take months. In contrast, voters want the votes tallied that night. Utahns would certainly not tolerate months of uncertainty around the counting of votes in a major election.

These four properties make Internet voting a very different proposition than other activities that we regularly undertake online. To see why, consider the problem of ensuring the integrity of the vote. Vote integrity is particularly important because people will not trust a government when they don't believe the results of the election are valid. The only reason we know about security breaches at Target and others is because their systems are, by design, transparent and auditable. Further, they are required by law to report breaches. Even if these companies were unable to prevent an attack, it was abundantly clear after the fact

---

[2] Danchev, Dancho. "Report: 48% of 22 Million Scanned Computers Infected with Malware." ZDNet. January 27, 2010.
[3] "House of Cards: Why Your Accounts Are Vulnerable to Thieves." Consumer Reports. June 1, 2011.

that a breach had occurred. In most Internet voting systems, however, the secrecy of the ballot makes the problem much harder than traditional systems for auditing and accountability.

Section 5: Potential Mitigation Strategies

Given that sufficiently secure Internet voting systems do not yet exist, they would need to be built. Of course, some systems, like a stone bridge to the moon, are impossible to build. Others, like a stone bridge to Hawaii, are so exorbitantly expensive as to remain a fool's errand. However, other systems, like spacecraft, aircraft, and the newer Sam White Bridge, are much more affordable. Unfortunately, with the four challenges mentioned in the preceding section, the unconstrained nirvana of Internet voting, "from any device, entirely online," is so impossible, or at least infeasible, as to be a fool's errand. At present, the notion that voters can vote from their personal device presents major challenges which need to be addressed and current technologies are limited in their abilities to address concerns delineated in this report; however, it might be possible to constrain the problem in a way that makes a solution entirely feasible, broadly appealing, and immensely valuable. We see two potential solutions:

1. **Online Ballot Construction (OBC)**. The state could build an online portal for voters to construct their ballots online, then print at home a human readable ballot with their vote, to be mailed in and processed as part of a broader and easier "vote by-mail" program. This approach requires the state to procure scanning equipment for reading votes from the range of papers and home printers used by consumers. The ballots in this approach would carry a cryptographically strong identifying number unique to each voter, but secret for that voter and sufficiently random in a numeric space that is big enough to ensure that guessing such numbers would be ineffective. This number would be used to ensure that each voter only mails one ballot and that no other party is "spoofing" or otherwise faking the voter's vote.

2. **Specifying Device Requirements**. Alternatively, Internet voting could be done entirely online if the voter's device met stringent requirements. This approach still requires construction of a strong "back end" server infrastructure, as well as strong device-side security, but such security is now possible on the device side of some of the more popular smart phones and tablets.

As we consider these ideas, and others, we should keep in mind each of the four challenges mentioned further above, and discuss the mitigation of each individually: Secret ballots are required; Computing environment is uncontrolled; Major elections are infrequent; The margin for error is very small.

Ballot secrecy makes Internet voting so much harder to realize than traditional online commerce. To make the online commerce scenario analogous to Internet voting, the shopping site would know that a

customer bought something, but could never tell anyone who did the shopping and what they bought or how much any shoppers spent individually except in aggregate with other shoppers. Further, to avoid voter coercion, it must not be possible to force a voter to demonstrate which way they voted. To see why this is a problem, suppose some group claims to have altered the results of an election after the fact. Whether they have actually done so or not is immaterial because there would be no way to prove whether or not they had done so, and the doubt cast on the election results represents damage in many forms. Voter confidence in the validity of the vote could be undermined without even going to the trouble of mounting an attack. Voter verification systems do not address this concern because it is very difficult to verify that a vote made it into the final count. End-to-end cryptographic verification systems can do this, but few commercially deployed systems have this protection, and the systems with cryptographic protection have not been adequately tested and validated. Fortunately, however, such security can be built into new Internet voting systems moving forward.

Traditional personal computers (PCs) do not have an architecture meeting security requirements for Internet voting. Fortunately most users now have a few different types of devices. Roughly 58% of Americans have a smartphone, and tablets are rapidly replacing desktop and laptop personal computers as 42% of Americans now have a tablet.[4] Many of these smartphones and tablets provide a hardware backed security architecture which would allow a sufficiently secure voting platform.

Unfortunately, with 48% of laptop and desktop computers infected by viruses, they do not make a safe platform for voting, particularly as most voters' PCs do not have the kind of hardware backed security technologies required for a sufficiently secure voting platform. However, the hardware architecture of most personal computers do not support hardware attestation, which could enable security vendors and voting software to make sufficiently strong claims on the security of the operation system on which they're running. In that context, we recommend excluding PC based systems from being eligible for Internet voting. Please note however, that PCs would still be eligible to participate in the Online Ballot Construction (OBC) whereby voters can print and double check their ballots at home before mailing the ballots into the county clerk.

In contrast, the State might achieve Internet voting by building a "sufficiently secure voting experience" with iOS and Android apps that run only on sufficiently secure hardware and operating systems, such as iPhones, iPads, and Android devices that can provide hardware attestation of their security. This enables most voters to use their own personal devices to vote. However, this does not support any standard browser. In that context, safely bringing Internet voting that is entirely online to voters in a reasonable timeline requires that we strike a balance sacrificing the ability to support any standard browser. We should also note that the proposed compromise still leaves election administration officials with a number of challenges and risks regarding the uncontrolled computing environment because the election administration officials do not control voters' iPhones and Android devices. Hardware based attestation in the mobile

[4] "Mobile Technology Fact Sheet." Pew Research Center.

device could be used to mitigate that risk, but that would be a leading edge approach, with all of the risks inherent to leading edge approaches .More research is needed to understand whether this option can truly supply secure internet voting.

If we spent money to procure a sufficiently secure voting system, then it would be a shame to use it only every four years. In fact, the technical and security staff operating the infrastructure will be more capable of professional operation if it is regularly exercised . Senate and local elections would add some regularity, but a single infrastructure serving multiple states would enjoy both economies of scale and the benefit from the improved execution. Practice and repetition, with a fully auditable infrastructure, are also crucial to decrease the margin of error. Security should be built in from the lowest level, including the hardware level, and each vote should be cryptographically signed as it is cast to ensure integrity at every step in the process, and the counting should be automated and entirely repeatable. Only by building such a solid infrastructure, and only through practice on smaller scale elections, can the error margins and security risk levels be brought down to levels anywhere near current “non-internet” voting systems.

Section 6: Security Recommendations

No system today can securely deliver broad capabilities that would allow voters to vote entirely online or from any device. However, dropping some requirements could potentially make it feasible to build a secure Internet voting system. We propose two possible approaches, but each compromises the benefits of Internet voting in favor of increased security. For example, relying on an application for Internet voting (instead of a typical Internet browser) would prevent some people from participating, and might disenfranchise them, and others, from voting altogether. Additionally, requiring the voter to install applications increases the possibility that voters can be tricked into downloading a counterfeit application. All such risks need to be mitigated in a strategy for Internet voting.

Election security is a national security issue, and must be treated as such. The legitimacy of representative democratic government depends on election security, both real and perceived. Anyone anywhere in the world can attack an online election, and they may be out of reach of U.S. law. Chance of attribution and being brought to justice are negligible. The system must be built from the ground up to resist such attack. There are a host of threats that need to be overcome through legal, procedural, and technical means if we want to conduct Internet voting in a way that continues to provide a trustworthy and reliable election system for Utah. Given the security problems outlined above, there are some specific goals that must be met by any system purporting to offer secure, Internet voting. The Computer Technologist’s Statement on Internet Voting[5] provides a convenient list as a starting place:

[5] "Computer Technologists' Statement on Internet Voting." Verified Voting.

- The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed to be free of malicious logic. Malicious software, firmware, or hardware could change, fabricate, or delete votes, deceiving the user in myriad ways including modifying the ballot presentation, leak information about votes to enable voter coercion, prevent or discourage voting, or perform online electioneering. Existing methods to lock down systems have often been flawed. Even if they were perfect, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.

- There must be a satisfactory way to prevent large-scale or selective disruption of vote transmission over the Internet. Threats include “denial of service” attacks from networks of compromised computers (called botnets), causing messages to be misrouted, and other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire selection or selectively disenfranchise a segment of the voting population. Fortunately, sound commercial means exist for mitigating “denial of service” attacks, but those means must be factored into the final solution for Internet voting in Utah.

- A system of checks and balances will be necessary. We must install strong mechanisms to prevent undetected changes to votes, not only to outsiders but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and/or data. Internal security and auditing are as, or more, important to securing a legitimate system.

- There must be a reliable, unforgeable, unchangeable voter-verified record of votes that is at least as effective for auditing as paper ballots without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the Internet but without paper is an unsolved problem. Furthermore, the entire system must be reliable and verifiable even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

We cannot recommend that Utah adopt Internet voting unless the chosen system is shown in open, public trials to achieve the preceding four goals. By “open” we mean that the challenge to break the system is available to all challengers. If a system is to be a general Internet voting solution, then it must be subjected to security tests in a mock election on the open Internet. Anyone must be allowed to mount an attack over a period of time similar to the time frame of an election.

We recommend that Utah build requirements for an open, public trial for any proposed voting system. The requirements should clearly state the level of integrity and auditability that is required for acceptance along with the overall security and integrity goals for the system. Be aware that even with open, public penetration trials, an Internet voting system would still be subject to malware, phony voter, DDoS, phishing, and insider attacks. So we further recommend that any requirements for an Internet voting system address these concerns specifically and require that vendors satisfy them. In addition, Utah should strongly consider that source code for the entire voting system be made open source so that it can be subjected to review, build, and test by computing professionals not under the influence or supervision of the vendor.

Section 7: Possible Applications of Internet Voting

Several studies have argued that new technologies like Internet voting should be implemented as pilot projects that are slowly expanded based on the results of these pilots. The two populations of voters typically considered best for such pilots are UOCAVA and individuals with disabilities. There have been multiple trials of remote Internet voting for UOCAVA voters, where voters cast actual ballots online. Similar pilot programs could be implemented in Utah.

The first of these efforts was conducted in 2000 by the Federal Voting Assistance Program. Since then, Internet trials focused on the UOCAVA population have been conducted in Arizona, West Virginia, and Okaloosa County, Florida.[6] In the 2010 general election, West Virginia allowed for remote Internet voting for its UOCAVA population. Its system worked as follows: when a voter submitted a Federal Post Card Application (FPCA) or a West Virginia Electronic Voting Absentee Ballot Application, a voter who supplied an email address received an email from the county clerk or one of the two voting systems vendors that contained a username and the name of the website where they could access their ballot. The voter then used their credentials to log onto the website where they could mark their ballot selections. The voter clicked a “Cast Ballot” button and the ballot was transmitted to the voting server. The voter then received a code that allowed them to check whether their ballot was received and processed. The code did not allow a voter to view their ballot choices again. Please note that this approach does not mitigate the security risks of malware that can both modify votes, and also modify what is presented to the user when they check whether their ballot was received and processed. However, it is a starting point for UOCAVA, even though it sacrifices security to increase anonymity compared to other UOCAVA approaches, but we would not recommend applying this approach to the broader set of Utah citizens who deserve both security and privacy, both integrity/accuracy of their vote, as well as secrecy of their vote.

Section 8: Policy and Legal Considerations

[6] See "A Survey of Internet Voting." by the U.S. Election Assistance Commission for a summary of all trials conducted prior to 2012.

We recommend making incremental legal and policy changes in our current voting process that would help voters and election officials prepare for Internet voting in the future. These changes include the adoption of online petition signing, emphasizing voting by mail, altering the voting equipment certification process, establishing voting identification cards, and general improvements to the voter registration system.

In 2012 the Lieutenant Governor was tasked to study how registered voters could sign petitions online. The study was completed and presented to the Legislature in 2013. The study suggests that creating an online platform for petition signing would not be difficult and would provide a benefit to voters, petition sponsors, and election officials. Implementing the study into a pilot project would give the Lieutenant Governor and election officials an opportunity to test some of the aspects of Internet voting. This may include a voter PIN, password for identification, and testing the auditability of an Internet voting platform.

Utah code requires that all voting equipment must be certified by the Election Assistance Commission (EAC). Political maneuvering in Washington DC and attempts to defund and eliminate the EAC have brought the certification process to a slow crawl. Some states have opted to remove the requirement for equipment certification, or move the certification process to independent accredited laboratories.

The secrecy and security of Internet voting can only be facilitated with an additional form of identification not currently available in Utah. This may include a supplemental voter identification card for voters wanting to participate in Internet voting, a chip and PIN card with password and card reader, or implementation of a digital driver license, similar to Iowa's test program.[7]

Harsher penalties for interfering with or impeding an election, specific to Internet voting, should be considered. The current penalties for violating election code range from a class A to class C misdemeanor. The most serious offenses, all class A misdemeanors, are electioneering, obstructing access to the polling location, removing ballots from the polling place, soliciting voters to show their ballot, and receiving or delivering ballots to a voter unless that person is a poll worker. Other violations include falsifying an absentee voter affidavit, influencing an employee's vote, or allowing your vote to be seen.

Utah Code, 20A-3-502, seems to be the most applicable to individuals who interfere with Internet voting. It states, "It is unlawful for any person by abduction or duress, or any forcible or fraudulent device or contrivance whatever, to impede, prevent, or otherwise interfere with the free exercise of the elective franchise of any voter…" The penalty for violation is a class B misdemeanor, generally a fine of up to $1,000 and jail time of 6-9 months. However, harsher penalties may not deter individuals who are outside the state or country. Cyber-attacks may originate from any country in the world, leaving the state without an option for punishment if a crippling attack occurred.

With Internet voting, a voter's browser would effectively become the polling location. Notices of election, sample ballots, information on voters' rights, and any other notices required by law to be visibly

---

[7] Schwarz, Hunter. "Iowa's Going to Have Smartphone Driver's Licenses." Washington Post. December 9, 2014.

posted at a polling location would need to be posted on the voting website, emailed to voters, or pushed via a smartphone application.

Policy updates would need to be considered regarding candidates who are disqualified for failing to file the appropriate campaign financial reports. The current requirement is to notify the voter by any means possible that votes cast for that candidate will not be counted, which is usually accomplished by posting signs in the polling location. Voters who vote by mail or cast a vote during the early voting period, prior to the candidate disqualification, often feel as though their vote has been thrown away. Participating internet voters would need to be notified before they cast their ballot. Allowing a voter to update their ballot after a candidate is disqualified has potential for a variety of harmful events. In the interest of election security, we recommend that they do not. Once a ballot is cast, the ballot is cast.

The current standards for size and design of paper and machine ballot formats are detailed in 20A-6, and include layout, labels, titles, font size, vote selection/oval/box, write-in lines, etc. These standards would need to be amended to meet current webs design and usability guidelines. Consideration should be given to standards for voting instructions that are simple to understand.

State election code defines specific opening and closing dates and times for early voting and by-mail voting. Internet voting would need to have similar policies enacted. The current deadline for UOCAVA voters to submit an electronic ballot, via an online ballot marking portal or by email, is 12:01 a.m. on the day of the election.

Currently, citizens can register to vote using a traditional paper application, the Driver License Division, or through the State's online voter registration website. Whichever method is used, the voter's information is entered into the Voter Information and State Tracking Application (VISTA) by election officials. A transition to Internet voting would require integration of a voter registration system that is accurate and more automated than the current system. Similar to the VISTA system used today, it would serve as verification of a voter's registration, their right to vote, which ballot they qualify for, and storage of vote history.

Policy that encourages a broader use of vote centers and voting by mail may ease the transition to Internet voting. Transitioning voters to a mail ballot will help shift the idea that voting must take place at an external location and move the voting experience into a voter's personal space at a date and time of their choosing. Voting by-mail would ease the cultural shift to Internet voting.

Current law prohibits any campaigning within 150 feet of a polling place. However, there are no current laws prohibiting electioneering online. If an individual's browser effectively becomes their polling place, political advertisements or pop-up ads could appear before voters as they cast their ballots. Online electioneering would be far more difficult to limit and restrict than electioneering around a physical polling place.

Other reports and experiences on Internet voting have demonstrated that years, not months, are needed to design, implement, and develop an Internet voting platform. Caution must be employed to ensure the complete security of the system to build and maintain trust with the voters.[8]

Conclusion

The Internet is becoming an integral piece of our daily lives. It is no surprise that the election discussion has entered this realm. Online shopping and banking are common events, but moving our elections may prove more difficult. Our findings in this report indicate that Internet voting has many advantages and may greatly benefit certain populations of voters, particularly voters with disabilities. These voters have the most potential benefits from Internet voting due to their difficulties with traditional polling locations. Making voting easier for citizens also proves to increase representation, which is a compelling interest in itself. Younger generations are showing to have less interest in government and as a result show less interest in civic duty. However, they are growing up with more advanced technologies and trust them more than their older counterparts. Internet voting may provide an avenue to attract youth to the electorate.

Another benefit in moving away from older technologies is maintenance costs they are incurring. The action in question is whether to invest in our older machines or look for alternative methods. The federal government will not be aiding the states in replacement machines or new improvements. Any election costs will be the states' responsibility for the foreseeable future. The condition of our poll workers is also worth note. As the current poll workers are aging, there are fewer replacements volunteering. Voters with disabilities require more attention from poll workers, and routinely do not receive adequate assistance. By reducing the number of poll workers required we can focus the supply to areas with more demanding needs. The final benefit of Internet voting is the ability to tabulate instant results. Recounts may be quicker and provide instant gratification to candidates and the public. This may seem unnecessary, but in today's culture of instant results we should not overlook the benefit. Internet voting will decrease administration costs by reducing the number of machines, by-mail paper ballots, and poll workers. Initial cost may be higher, but long-term, our current system is not sustainable.

The problem is that Internet voting also possesses numerous inherent security risks that must be mitigated before it is implemented. An election requires legitimacy, accuracy, and ballot privacy. Weak security in any of these areas will attract attention from those whom have malicious intent. Security compromises among large corporations give us an example of potential problems, and while these companies may accept these problems as the cost of doing business, an election cannot. These companies also have the advantage of running continuously. A system can quickly identify problem areas and bugs before they become extensive. Elections, on the other hand, will only be held roughly twice a year leaving

[8] Alternative Voting Technologies Report: Chief Electoral Officer's Submission to the Legislative Assembly. Toronto, Ontario, 2013. 20.

administrators and technicians limited time to react. The last security risk for Internet voting is accountability and auditing. Traditional voting systems provide paper trails and chain of commands that would not be readily available to an online system. No current system available addresses these risks.

If the legislature chooses to experiment with Internet voting, then we will need build it from the ground up. While extensive, there are possible solutions. An Online Ballot Construction (OBC) would, in theory, expand a vote-by-mail type of system to an electronic version. Specifying device requirements is also possible, but would need more infrastructure construction. Traditional personal computers do not have the security requirements needed, but could be used with an OBC system. Another possible solution is developing an application. However, there is a possibility this may exclude some potential voters or attract counterfeit apps. Regardless of which system we decide to use, it will need to include a few key aspects. First, the security aspect must address potentially modified ballots, online electioneering, and voter coercion. Second, it will need to prevent or account for Internet disruption. A voter unable to submit their ballot is not fair system. Third, provide auditing and accountability for outside and inside attempts at circumventing or undermining the system. Finally, a rigorous testing process is necessary to find bugs and defects. Any new system would need to be thoroughly tested through open, public trials that invited hackers and others to test the system and by introducing the system in pilot projects limited in scope.

Significant policy changes would also need to be implemented by the legislature. Several sections of Utah's election code would need to be altered to accommodate Internet voting. Online petition signatures may be an avenue to test potential programs. Possible defects could rise in a first-step type of program. Voters may also learn to adapt to the larger concept of Internet voting if they participate in smaller scale online petitions. Additionally, more identification may be necessary to secure access for voters. Harsher penalties would be needed due to the potential problems violators could cause. Violations coming from outside Utah or the United States may cause problems for prosecutors regarding jurisdiction. Notices will need to reach voters in a timely manner. This includes notices of disqualifications. A vote for a disqualified candidate is basically a non-vote. Finally, a more accurate registration process would need to be implemented. Currently voters may register online, but clerks have routinely noticed mistakes that usually are fixed by contacting the voter.

We urge the legislature to carefully consider the risks and the benefits of Internet voting, and, if the legislature chooses to implement Internet voting, establish a system cautiously to ensure that elections are run with integrity and fairness and that voters may adapt to the transition.