Jon Misevicz

Digital Voting

**Perceptions and Status of Online Voting**

One decade into the 21st century and some are wondering in an age where secure online banking and shopping have become common place the process of voting seems to be stuck in a state from a previous generation. There have been attempts at modernizing the American voting system at times attracted the attention Congress after incidents such as the Hanging Chads of the 2000 presidential election (Herrnson 2005). These attempts have met with varied success and additional controversy from citizens and various political agendas. Although some would like to believe that they can stymie the relentless process from moving forward some may find themselves overwhelmed by the pressure brought from successive generations (Duncan 2012).

From the varied attempts at electronic voting there have emerged three front runners which have captured the majority of attention. These all have issues surrounding them but have started to mature into viable alternatives to the current system. The primary method is already in place in some states which is the process of making the current system electronic via a touch screen or by computerizing the current ballot at the polling station. (Ellott 1998). On the other extreme is the attempts at removing the paper ballot in its entirety via a secure online voting website similar to modern shopping sites that have already been tested in various elections and across one European country. Somewhere in the middle is the compromise which allows voters to fill out a ballot then both download/print it and mail it electronically or though the postal system.

The problems with electronic voting can be distilled into a few topics which typically end up steering any debate. The technology surrounding each of the three systems have their critics and supporters. Most have been tested and shown to have weaknesses that need to be addressed to become viable options for the county. There is the little addressed problem with the perception surrounding the understanding of each system. The generation that has the consistent voting pattern according to polls tends to be the groups who drive the policies toward voting procedures. With that in mind it has been said that standards and the voting technology seems to always be a few generations behind where business is.

Each set of problems tend to have roots either in the unique way the constitution and congress have created election law or on the platform which the technology has been built. The problems discussed are not new, some of them going back to the first look at electronic voting (Subberlefield 2004), but the issues have not been resolved yet to the satisfaction of the general public. The current state and case studies show the viability and weaknesses of each example. This doesn’t mean that the current process is stuck in neutral and not going anywhere. As the current crop of young voters matures, and becomes a strong delegation, the relentless march toward fully electronic voting will come to fruition.

**Voting at the Polling Station**.

The most simple and currently implemented solution for voting is to replace the aging voting machines with modern touch screens or a method that fills out the ballot via a printed paper copy. With the passage of the Help America Vote Act in 2002 after the Florida hanging chad incident which shined the national spotlight onto issues with the in use voting technology. Congress made funds available to upgrade and update voting equipment, and digitize the voter registration database (Caton 2012). This was a boom for some private companies who took on the challenge of creating voting software, and after a few years Diebold emerged as the nation frontrunner.

This version of electronic voting meshes well with how voting is regulated. Even in national elections each state, at times each city, and district can have its own set of voting regulations that need to be followed. The procedures for voting are not set forth at the national level which presents issues when trying to modernize the voting system as it has to be extremely adaptable, easy to use and low cost as not to put undue burden on local municipalities. This also addressed one of the major fears by most voters over the digitization of the voting system, which would be the accountability of a paper trail.

The electronic voting system in this method typically has a touchscreen and the voter is lead though various options which then either prints out a ballot or records the ballot electronically onto a memory card. The touch screen itself has caused one of the two major issues with this system. In a video from the 2012 presidential election a touch screen is shown selecting a candidate which is not the one selected. This video was posted to YouTube and eventually was classified as viral after being picked up by the national media. The issue was quickly addressed by calibrating the screen but the damage to the perception of the touchscreens was already done as it sapped citizen confidence in the system.

The other notable incidents are far less easy to address in which either memory cards containing votes went missing or were shown to have incorrect tallies. The trouble with this situation is again it shows that with an electronic system that mimics the current paper system the same accusations of voter fraud can be made, as well as pointing the finger at privately created software. The issue centered around privately created software where the public cannot know how their vote is being recorded, indexed and eventually counted gave rise to a call for an open source voting system.

An open source voting system appealed too many because it seems to be centered on the idea of transparency. The community surrounding current open source projects has shown that they can be accurate, diligent and produce a working product. One of the benefits some see to open source programming is that currently 80% of the voting software is controlled by two companies. (Zetter 2009). This troubles many who view the open source code as superior as it is open for all to see, to improve upon and the down side, to hack. Although the latter is not unique to open source programing as demonstrated by a University of Michigan attack during a testing phase of a Washington D.C. voting system. The students were able to download voter information, change votes and even update the software, which they made play the University’s fight song. (Bjerg 2013) This being a test showed that the technology, although reaching maturity, is still very young and vulnerable.

To make this type of voting system work it needs to be secure, easy to use, have integrity and leave an audit trail. To secure the device it should be locked down physically with no ability to connect an external memory card. This could be simply soldering the memory directly on the board which then will be audited after the polls close. Using an open source software would give the impression of integrity as anyone could view how the votes are counted, and has been shown to be easy to use. Currently 16 states – Including many swing states, have no paper backup systems (Clayton 2012). The audit trail is the final bit which could make use of the reliable scanning systems that districts already have, but printing out a paper ballot which can then be verified by the voter, and scanned in a similar process which would be familiar.

The impression left by nationally reported embarrassing incidents has left a sour taste in a generation regarding this technology. Although with the Help America to Vote Act, this technology is in place in many states, there is starting to be a backlash against the system. (Klimas 2012). Florida, New Mexico, Michigan and Washington State have passed legislation requiring the use of the paper ballots, but have not rebuffed the technology altogether. There appears to be more of a wait and see approach, and with districts being strapped for cash it may make way for one of the other options, which tend to be cheaper.

**Digital Vote by Mail**

The ability to download a form from a government website which can then be filled out and mailed electronically or physically to a polling station to be counted is not a new one. This is one of the suggested methods put forth in a study in the 1990’s as the dawn of the digital age. The system this creates is familiar enough with most citizens to be viable but has its own share of public disappointments. This method has both the appearance of privacy because the form can be downloaded at home and then mailed but the last portion of that process is what the Achilles heel of this process is.

The idea that each district would create their ballot in a digital format and forgo printing thousands of ballots saving money, and preserving the ability to print on demand for those who feel more comfort voting in the traditional methods. Once downloaded or printed, depending on the final delivery method, the voter then fills out their ballot. They can then sign it physically or with a digital signature and return it to the polling place. The process seems simple, and logical and was adopted for a large scale implementation by the U.S. Military for solders overseas. The test has also worked in the smaller state of Hawaii which has been using the system since 2009 and plans on being 100% digital in nearly all aspects by 2016 (Kalani 2012).

The military has as much mixed results as Hawaii had successful results which shows that this method is still in a transition phase. There is no consensus as to how one could secure a digital vote, which then has to be emailed? How and where would it go? During the 2012 election there were rumors on local levels that some voters were getting rejected emails because the election processer’s inbox was filled. The question is also raised as to voter fraud where someone could just flood with duplicate ballots, and this could invalidate the legitimate vote. When sending through the mail from overseas, or another country the ballot would be open to possible fraud, not to mention going through foreign governments postal services.

These are still a small segment of voting policies and appears to be destined for local elections and may not get the critical mass for the national stage. It gives the perception to younger voters as being already too old where the technology has moved past this stage years ago. Older voters still prefer to go into the polling place and the newest voters would rather vote via their smartphones (Duncan 2012). In the long term this may be more of a bridge technology as others mature faster.

To make this technology viable, one would have to consider the long-term investments. Technology pace already suggests that a more mobile citizenry will demand a versatile voting platform (cite source). Yet the benefit of being able to print off a ballot as needed during an election if a polling place runs out, and the ability to reach disabled voters remains quite high. Being able to email securely seems to be the other major hurdle which can be easily solved by using a blind signature type technology. This method of cryptology is high secure and provides anonymity for a vote. The ballot is first ‘blinded’ making it anonymous and then signed by using a public key. That way both the public cryptographic key and the blinding algorithm can both be used to verify each other making it nearly impossible to crack over standard internet. (Blind Signature, 2013). The advancement toward this method of electronic voting appears to be too late in the game to be a very viable alternative to traditional voting though.

**Vote over the Internet**.

There have been many attempts to start the truly digital format of voting over the internet, but to date there isn’t one that has been able to overcome the controversy. The traditional model of online voting would be similar to accessing your bank account. A government or privately held company would verify your identity and allow you access to a secure voting site. A citizen then could fill out their ballot, either from the comfort of their home, at the office or even sitting in a coffee shop. Once the ballot is filled out it would be automatically entered into the official record. This last portion of the process is also the most criticized, as it doesn’t leave a paper trail.

The problem with online voting first comes down to how you identify the voter. Estonia has already successfully implemented a complete national online voting system for the 2005 elections (Borlan 2007). This is aided by the national electronic identification card which isn’t an option for the United States. The argument then is typically drawn along the lines that we can bank, and pay for goods securely, why can’t we vote online? This is a good point because those systems completely identify a person, link their transaction histories, and track the individual. One of the corner stones of American voting is that no one knows who you vote for, the anonymous value we place on elections. There isn’t a viable solution yet to reach a consensus on how to resolve this issue.

When a system once identifies you as an eligible voter, then your ballot can be tailored to your district. This is often one of the bullet points when referring to the cost savings and ease of access. What if you couldn’t get to the site, how do you know that the site you’re on is legitimate? During an election a group of hackers could issue a Denial of Service attack against the web server making it impossible for a citizen to vote. One possibility using this type of situation could be what is known as a Man in the Middle attack. (Gallagher 2011) This is where a hacker could reroute your already verified vote to another site giving them the ability to steal your identity and maybe even cast your vote for you.

How likely is this to happen? One could never know with certainty because currently there is no national requirement for a paper trail when using online voting. The constitution of the United States leaves it up to the states to decide how to run elections. To bring about a national voting system there first must be a consensus within congress to pass voting legislation which typically cannot garner enough support. There is also not complete online access in all corners of the country which would bring up the often cited claim of disenfranchisement. Until there is enough critical mass toward a universal system there will not be the political capital for lawmakers to lead instead of protecting the status quo.

**A Possible Solution**.

The need to modernize the current election system is gaining ground with every election. As the citizenry ages, new voters who have never grown up disconnected will start to demand change. There may be hope to gradually ease the U.S. instead of a rallying cry which will then bring by a legislation which could cause more harm than good. To accomplish a digital voting system, it first must be secure, and this security should be nearly transparent. It should also be easy to use, with the ability for states to adapt it to their own ‘blend’ of polling. Finally, it must have integrity to pass the public’s already tarnished perception of computerized voting.

To bring about the security needed to provide an anonymous yet traceable voting system we can use technology already in place. The tricky part is keeping the vote anonymous, but this could also be how it is looked at. Already, the U.S. has a system in place that in theory tracks all citizens for taxation purposes. An individual’s social security number is a perfect example of a government’s ability to identify citizens. The keep the authentication system secure it would act as a clearing house similar to the way credit card companies authorize transactions. A simple tally could be flipped as well as a transaction record signifying that a vote has been cast, not who it was cast for. Using military level encryption as well as independent public and private monitors during the election would ensure a level of accountability. “The data is critical. Don’t take shortcuts. Use good, best-of-breed, standard based security” (Jackson, 2012)

Making access available for all voters is another dilemma. To accomplish this the procedure can use a hybrid of all the systems. The authentication clearing house stated above could be used to identify voters who go to the poles, or vote online. There wouldn’t be the need to run multiple systems and could help ease the costs to local districts. Using an open source standard for voting programs could aid in the development of easier to use software, while still allowing private companies the ability to design front end interfaces while offering physical secure machines. By having it open source, similar to the development of the Linux operating system, a level of technology transparency exists where no one company owns the rights to an American’s ability to vote.

Maintaining integrity is critical for any voting system to pass the public’s perception of infallibility. The demand for a paper trail in addition to the electronic vote can be ensured the same way we currently do with online shopping. A simple digital receipt with a transaction number would be generated, and at physical machines the ability to print a ballot or receipt would suffice. By using the government’s own security provided by high level encryption the election is secured in the perception that it could not be tampered with. The downside to this system is that any little incident has the potential to bring ruin to it. To counter this type of situation the government would have to provide quick, and honest answers to any situation. In a golden system it could even open up the digital voting records by district with no name attached for analysis by any citizen.

From all the examples cited, a single critical path to success still remains murky. The process for proving a national system of voting would rely on leadership not technology. The current ability of off the shelf and military encryption can provide the security. The far reaching community who support open source software has already started to develop a voting system (Klimas 2012). The voters coming of age in this latest generation have grown up having a smart phone in their hands and are already questioning the very ability to vote electronically, and their voices are only going to get stronger. It is that voice, the voice of a concerned vote which will eventually lead to a revolution, or one could say the acceptance of computerized voting.

**Works Referenced**

Blind Signature (n.d). Retrieved June 30, 2013 from Wikipedia. Wiki: http://en.wikipedia.org/wiki/Blind\_signature

Bjerg, Alexandra (Feb 2013). Path toward online voting stymied by fear of hacking. CAFWD Org. Retrieved from: http://www.cafwd.org/reporting/entry/path-toward-online-voting-stymied-by-fear-of-hacking

Borlan, John (Feb 2007). Online Voting Clicks in Estonia. *Wired.com*Retrieved from: http://www.wired.com/politics/security/news/2007/03/72846?currentPage=all

Caton, Josh (Oct 2012). How Close are We to Internet Voting?. *Mashable*. Retrieved from: http://mashable.com/2012/10/02/internet-voting/

Clayton, M (July 2012). Is Your Vote Secure? Many digital systems lack paper backups. *Christian Science Monitor*. Retrieved from: http://www.csmonitor.com/USA/Elections/2012/0727/Is-your-vote-secure-Many-digital-systems-lack-paper-backups-study-says

Duncan, Geoff (Nov. 2012). It’s the 21st Century! Why are we not voting online yet? *Digital Trends****.*** Retrieved from: http://www.digitaltrends.com/mobile/its-the-21st-century-why-arent-we-voting-online/

Elliott, David (June 1998). Examining Internet Voting in the State of Washington. [Power Point Slides] *Office of the Secretary of State****.*** Retrieved from: http://www.sos.wa.gov/elections/evoting\_paper.aspx

Gallagher, Sean (Sept 2011). Diebold voting machines vulnerable to remote tampering via man-in-the-middle attack. *Ars technical*. Retrieved from: http://arstechnica.com/business/2011/09/diebold-voting-machines-vulnerable-to-remote-tampering-via-man-in-the-middle-attack/

Herrnson, Paul S. (2005) Beyond the Hanging Chad: The Promise and Performance of Electronic Voting. *University of Maryland****.*** Retrieved from: http://www.csmonitor.com/USA/Elections/2012/0727/Is-your-vote-secure-Many-digital-systems-lack-paper-backups-study-says

Jackson, William (2012, Nov 02). Securing voting machines is only half the battle. [Web Log comment]. Retrieved from: http://gcn.com/blogs/cybereye/2012/11/voting-machine-security.aspx

Lohrmann, Dan (May 2009). Honolulu’s Internet Vote Worked: The Wave of the Future. *Solutions for State and Local Governments*. Retrieved from: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Honolulus-Internet-Vote-Worked.html

Kalani, Naema (May 2012). Hawaii Voter Registration could be online by 2016. *Honolulu Civil Beat****.*** Retrieved from: http://www.civilbeat.com/articles/2012/05/08/15763-hawaii-voter-registration-could-be-online-by-2016/

Klimas, Liz (Nov 2012). Why are some states dumping their electronic voting machines and going back to paper? *The Blaze*. Retreived from: http://www.theblaze.com/stories/2012/11/01/why-are-some-states-dumping-their-electronic-voting-machines-and-going-back-to-paper/

Subberlefield, Adam. Rubin, Aviel. Wallach, Dan. Kohno, Tadaysohi. (Feb 2004) Analysis of an Electronic Voting System. *IEEE Symposium on Security and Privacy.* Retrieved from: http://avirubin.com/vote.pdf

Zetter, Kim (Oct. 2010). Nations First Open Source Election Software Released. *Wired*. Retrieved from: http://www.wired.com/threatlevel/2009/10/open-source/