# e-Voting in America: Current Realities and Future Directions

Nathan Johnson[1(✉)], Brian M. Jones[2], and Kyle Clendenon[2]

[1] Western Carolina University, Cullowhee, NC, USA
jnjohnson@wcu.edu
[2] Tennessee Technological University, Cookeville, TN, USA
bjones@tntech.edu, kclendeno21@gmail.com

**Abstract.** This paper presents a snapshot of the current status of voting methodologies in the United States as of November 2016. The authors present the methodologies currently employed to facilitate voting including paper based and direct recording electronic systems. This is followed by a discussion of voter confidence in the election system where e-voting systems are utilized, particularly in the areas of auditing, security, influence, and human-computer interaction (HCI). The paper concludes with a brief summary of the future of e-voting, including what technology is on the horizon, and a discussion of future research directions.

**Keywords:** e-Voting · Human computer interaction · Election process · Voter confidence

## 1 Introduction

Ever since Alexander Hamilton first wrote about "the mode of appointment of the chief magistrate of the United States" in Federalist No. 67 [19], and George Washington was elected their first president in February 1789 [30], citizens of the United States (US) have been electing their governing officials. The president, governors, senators, congressional representatives, judges, mayors, and local officials have all been selected through the process of free and open voting.

Americans go to the polls nearly every year to vote for something, whether in local, state, or national elections. Although this exercise in democracy has been carried out unchanged since the early days of the republic, the method in which the votes are cast has not. In fact, as technology has advanced, so has the manner in which voters cast their vote. Technology has allowed the voting process to become more streamlined and efficient, and given rise to a variety of interfaces in which the voter may find themselves facing on Election Day. Along with these technological changes have come challenges in recording and tallying votes, and with these challenges, issues of trust in the voting system. Many of these challenges have presented themselves in the most recent US national election of President Donald J. Trump.

In the following pages, we review the different voting methodologies currently employed in the US and highlight the human computer interaction (HCI) considerations where appropriate. Next, we discuss how voter confidence in the election process

G. Meiselwitz (Ed.): SCSM 2017, Part I, LNCS 10282, pp. 337–349, 2017.
DOI: 10.1007/978-3-319-58559-8_27

has been affected in terms of auditing, security, influence, finances, and HCI. Finally, we report on the future of voting technology, and offer further research direction.

## 2 Current Voting Systems Utilized in the United States

Voting systems in the US have varied from polling place to polling place over the years. These voting systems consist of various hardware, display devices, and methods for collecting and storing voting data (Roth [42]). In some states, such as New Mexico, Montana, and Maine, the voter encounters a system that Abraham Lincoln would find familiar - a paper ballot filled out and then counted by human hand. In three states, Washington, Oregon, and Colorado, and several counties in other states, voting is executed via the US Postal Service mail on paper ballot. In still other states, votes are cast and tallied on what are referred to as Direct Recording Electronic Systems (DRE), a completely electronic touchscreen and tallying system. Two systems, the punch card and mechanical lever, once mainstays across US polling places, have now been completely discontinued as methods for voting.

As of 2016, a mixture of these systems exist across the US, even differing from county to county within the same state in some cases. In addition, some of these systems allow for an audit of the actual vote and others do not depending on the system and the proprietary nature of the vendor supplying the system. In the following paragraphs, we detail how voters interact with the different voting systems currently used in the US [46].

### 2.1 Optically Scanned Paper Ballot System

When using paper ballot systems, voters typically mark their selections by filling in a space on a paper ballot (similar to an academic test scantron form). It is usually a box, oval, or circle that is completely colored in by the voter. Once all ballots are filled in and voting is complete, the ballots are electronically scanned and tallied to determine the number of votes cast for each candidate. Mail in voting occurs via this method in addition to traditional polling place voting. These ballots are typically auditable and able to be recounted by hand if necessary. As of 2016, nearly three-quarters of the US still uses this type of voting system [3].

### 2.2 Direct Record Electronic System

DREs are electronic systems that employ computers to capture votes immediately into an electronic memory module. There are various types of DRE systems, and interfaces may include touchscreens, electromechanical dials, and even buttons that are pushed to register the individual voter's selection. All votes are stored by the computer on a memory device (usually an internal hard drive). Some DRE systems are equipped with printers that allow a print out for the voter to confirm that their vote was inputted into the system as they wished before it is saved to the storage device. In addition, having a printout serves as a paper record of the vote providing an audit trail. However, not all

DRE systems are auditable and provide no means to determine if votes were missed, inaccurately tallied, or recounted.

### 2.3 Ballot Marking System

Ballot Marking systems are used to help disabled voters have easy access to voting technology. These devices generally use a combination of touchscreen and audio or other element such as gesture interaction, eye tracking, or other accessibility feature. These systems typically capture the vote on a paper ballot of some type, and the vote is later tabulated and recorded manually by humans. These types of systems are fully auditable and provide a method of recount.

### 2.4 Punch Card and Mechanical Lever Systems

These voting systems were once ubiquitous across the US and found in many polling locations, but as of the 2016 election season, they have been completely phased out [45]. These systems were retired after passage of the Help American's Vote Act (HAVA) in 2002, a response to issues discovered in the 2000 Presidential election where over a million ballots were not processed correctly [29]. Punch card voting systems utilized a paper card and a small device that allowed voters to punch holes in the ballot card corresponding to their desired vote. The pattern of holes punched indicated what candidate(s) the voter chose. Once the entire ballot card was completed, the voter then deposited it into a secure box to be tabulated later - either mechanically or by hand.

Punch card systems were not used as of the 2016 election cycle. Mechanical lever systems were first introduced in the last decade of the 1800s and were used in multiple jurisdictions across the states throughout the 20th century [32]. Voters utilizing mechanical voting machines would enter a booth and slide a mechanical lever to one side revealing their voting choices. Voters would then pull knobs to make their choices. Once complete, the lever would be slid back to its original position and the votes would be cast [6]. Mechanical lever systems have not been used since the 2010 election cycle.

In Table 1 below, the different voting methods and voting audit availability by state are reported [46].

## 3 Voter Confidence in the e-Voting Process

Using a combination of the voting tools outlined in the previous section, US voters have regularly gone to the polls to vote for their respective candidates since the late 18th century. Although the number of Americans going to the polls since WWII has dropped by nearly half [26], the free exercise of voting and the notion of being governed at the consent of the voter has endured.

Although the process of elections have persisted throughout US history, every election cycle generates episodes of vote miscounts and recounts, voting machine problems, vote tampering, precinct worker misconduct, and instances of voter fraud

**Table 1.** Voting methods by state

| State | Voting method | Auditable? | State | Voting method | Auditable? |
|---|---|---|---|---|---|
| AL | Optical scan paper ballot systems | Yes | MT | Optical scan paper ballot systems | Yes |
| AK | Mixed paper ballot and DRE systems | Yes | NE | Optical scan paper ballot systems | Yes |
| AZ | Mixed paper ballot and DRE systems | Yes | NV | DRE systems | Yes |
| AR | Mixed paper ballot and DRE systems | No | NH | Optical scan paper ballot systems | Yes |
| CA | Mixed paper ballot and DRE systems | Yes | NJ | DRE systems | No |
| CO | Mixed paper ballot and DRE systems | Yes | NM | Optical scan paper ballot systems | Yes |
| CT | Optical scan paper ballot systems | Yes | NY | Optical scan paper ballot systems | Yes |
| DE | DRE Systems | No | NC | Mixed paper ballot and DRE systems | Yes |
| FL | Mixed paper ballot and DRE systems | No | ND | Optical scan paper ballot systems | Yes |
| GA | DRE systems | No | OH | Mixed paper ballot and DRE systems | Yes |
| HI | Mixed paper ballot and DRE systems | Yes | OK | Optical scan paper ballot systems | Yes |
| ID | Mixed paper ballot and DRE systems | Yes | OR | Optical scan paper ballot systems | Yes |
| IL | Mixed paper ballot and DRE systems | Yes | PA | Mixed paper ballot and DRE systems | No |
| IN | Mixed paper ballot and DRE systems | No | RI | Optical scan paper ballot systems | Yes |
| IA | Optical scan paper ballot systems | Yes | SC | DRE systems | No |
| KS | Mixed paper ballot and DRE systems | No | SD | Optical scan paper ballot systems | Yes |
| KY | Mixed paper ballot and DRE systems | No | TN | Mixed paper ballot and DRE systems | No |
| LA | DRE systems | No | TX | Mixed paper ballot and DRE systems | No |
| ME | Optical scan paper ballot systems | Yes | UT | DRE systems | Yes |
| MD | Optical scan paper ballot systems | Yes | VT | Optical scan paper ballot systems | Yes |
| MA | Optical scan paper ballot systems | Yes | VA | Mixed paper ballot and DRE systems | No |

(*continued*)

**Table 1.** (*continued*)

| State | Voting method | Auditable? | State | Voting method | Auditable? |
|---|---|---|---|---|---|
| MI | Optical scan paper ballot systems | Yes | WA | Mixed paper ballot and DRE systems | Yes |
| MN | Optical scan paper ballot systems | Yes | WV | Mixed paper ballot and DRE systems | Yes |
| MS | Mixed paper ballot and DRE systems | No | WI | Mixed paper ballot and DRE systems | Yes |
| MO | Mixed paper ballot and DRE systems | Yes | WY | Mixed paper ballot and DRE systems | Yes |

***Source:*** [46]

and/or disenfranchisement of a voting block. The most recent US presidential election was no different. For instance, in Connecticut, ballots were used that had the wrong candidate listed for the state legislature. Those ballots were used for over an hour before the error was caught [31]. In Georgia, North Carolina, and Pennsylvania it was reported that DREs were ‘flipping’ the vote from one presidential candidate to the other whenever the voter tried to select their favored candidate [9, 14, 44]. And in Michigan, scanning systems in over one-third of the all the voting precincts in Detroit recorded more votes than should have been possible for that particular precinct [28].

One of the impetuses for advancing e-voting technologies has been to streamline and strengthen the voting processes, while further empowering the citizenry [8]. For the most part, this has occurred. However, even with the passage of HAVA, and as the above reported scenarios from the most recent election cycle highlight, several considerations are still at play when discussing how confident the populace is in e-voting systems and methodologies. We believe that these considerations can be grouped into one of five broad categories: auditing, security, influence, finances, and HCI.

## 3.1 Auditing

A primary issue with e-voting on DRE machines is the potential lack of auditing the vote. While some e-voting machines allow for paper trails to be generated, others do not. Further, an auditing function is not required by the Federal Election Commission (FEC), although some states have enacted their own auditing rules. This lack of paper trail for every vote cast leaves the voter with the possibility of being “disenfranchised” if there is a contested election or some form of recount because there is no record of how they actually voted if they use a DRE that doesn’t provide a paper receipt or is capable of a simple vote audit.

Complicating the issue is the fact that DREs are all proprietary pieces of machinery manufactured by a corporate entity. This reality carries with it the need for privacy and secrecy in testing and certification of the machinery. Both the tests and the results are often closely held secrets by the manufacturing entity, and tests only check for compliance with minimal FEC requirements. Further, any software running in the DRE that is considered commercially available is not required by the FEC to be tested [43].

### 3.2 Security

If auditing is the first issue that tops the list of voter concerns with DREs, security and integrity of the vote is a close second. Malicious tampering with a DRE system is a possibility both while the machine is in storage, or while it is actually being used to vote with. A report by the Congressional Research Service found that DREs are subject to a variety of nefarious attacks, particularly from malicious code [16]. These types of code (malware, viruses, Trojan horses, etc.) have been shown to be able to exploit themselves within machines and transmit to other linked machines. In addition, exploits based on basic memory buffer and encryption errors have been shown to be possible on certain vendors' machines [7].

One scenario of malicious tampering might find code being introduced physically via a bad actor while actually voting via some form of direct input or tampering. Another scenario sees the bad actor using innocent voters to carry out the attack on the DRE. For instance, some DREs require a "voter card" be used to activate the voting instance. These cards are reused by different voters throughout the election cycle. If one of these cards was stolen, compromised, and then reintroduced to the voting environment, unsuspecting voters might inadvertently introduce malicious code into the system. These so called "air gap" attacks have been demonstrated to be effective and quickly carried out. Attacks may do something as straight forward as altering vote tallies for particular candidates, or something more stealthy such as changing votes to specific candidate in a somewhat random fashion in order to disguise the nature of the attack. Even more sinister, some attacks might display one candidate on the screen, but record the vote for a different candidate [27, 48].

Other possible scenarios include compromising the central voting database used by the county or precinct that "programs" the DREs and collects the data from them as votes are tabulated. This intrusion could come physically or remotely as these central databases are often connected to the internet. Frustratingly, many of the DRE systems used around the US are running on software that only interfaces with now-extinct software such as Windows 2000 and Windows XP, the former of the two operating systems not having a security update in over six years.

A dilemma of security lies in the fact that every precinct and every state could be, and in some cases are, conducting their elections using different processes and systems. There are no set standards for security or nationwide policies that dictate how DREs are stored, activated, and used. Although, many have pointed to this very confusing and seemingly out of control arrangement, this decentralized and eclectic methodology for voting state by state, as part of the strength of the overall system. Because there are no set standards or common ways of conducting elections from state to state, it makes a coordinated attack on the entire system virtually impossible [33].

### 3.3 Influence

Another issue that surrounds e-voting is one of influence. As noted previously, DRE machines are acquired from a variety of vendors. The technology, software, and methodologies that these machines use to capture voter input may differ from county to county in the same state. Since each vendor has their own proprietary technology, issues surrounding trade secrets and industrial espionage make independent reviews of systems difficult [7]. Since a total air of secrecy surrounds these machines, voters are often left to wonder who is behind the companies that are providing the machines and doing the requisite testing to ensure they are working properly.

An informal interview with 20 recent voters showed that most felt fairly confident in the voting system in general; but when asked specifically about electronic voting, 3 of them expressed uncertainty in the "security" of their vote. They implied that it would be easy to change votes or simply not count votes, even with the checks and balances in place. Interestingly, 15 of the 20 participants felt that some undue influence was attempted on the most recent Presidential election. Most expressed that influence was always exerted in some way through money and power but that this year Russia might have also tried to influence the results.

We can see in the last US presidential election a prime example of the outside influence problem that voters have with electronic voting (and perhaps with voting in general in the US). Several news outlets, political blogs, and social media feeds reported on the connection between world-renown billionaire George Soros and the company Smartmatic that makes DREs. The story had little to no effect on the outcome of the election as no DREs from Smartmatic were used in the 2016 election cycle [10]. However, the story did highlight the potential for many voters to wonder if they could be confident that their vote was actually being cast for the candidate they wanted when using a DRE.

### 3.4 Finances

Many states took federal HAVA funding in 2002 to buy e-voting equipment, but have been unable to fund their replacements. Georgia, for instance, is using systems 10 years beyond their life expectancy and are not going to be able to replace them until the 2020s [41]. In 2007, the State of California announced that all of its DREs were to be pulled from service because they had failed simple security audits. Due to San Diego County's fraud, waste, and abuse rules, they were unable to dispose of the "useless" DREs and had to put them into storage. They have been paying the bill to store unused DREs ever since. Many of these voting systems come with annual "service" fees that cost the customer many times over what was paid for the original equipment. And still other systems are sold using antiquated technology inside such as ZipDrives, for which you can no longer even purchase media.

The problems and concerns facing e-voting in the US should probably be those of technology, security, and reliability [43]. Due to problems raised above surrounding auditing, security, influence and finance, e-voting has become a political football, a source of overall mistrust in the election process, headaches in the precincts where it is employed, and the go-to scapegoat for election night problems, voting challenges, and outcome disappointments.

### 3.5 HCI Considerations

In addition to the more intangible issues surrounding e-voting, there are also some physical and user interface considerations that must also be addressed for the electorate to continue using and supporting e-voting methods. Simple decisions regarding the design of e-voting interfaces can affect the outcomes of elections [47]. Seemingly simple design choices can affect how a voters choices are selected and recorded [13]. For this reason alone, it is vital that DRE interfaces are simple enough that it's very difficult for the voter to not understand how to use them [34]. Making DRE interfaces simple should help increase the public's acceptance of the technology [20]. In addition to simplicity, voters must feel that the e-voting system is usable. One of the main tenets making a computer system usable is its ability to make the user feel as though their use of the system will result in the intended effect [39], and if that effect is not achieved, there will be a mechanism for amending an action to achieve that effect [15].

Although we live in a techno-centric society, not everyone is computer literate or even wants to deal with technology [35, 36]. DREs should be designed with intuitiveness in mind, as users may not be accustomed to interfacing with technology. A recent study found that a significant number of voters in Georgia and Maryland, particularly those more advanced in years, required some form of assistance in order to successfully cast their votes [13].

In addition, age begins to affect other faculties such as vision and strength. Voters aged 52 and older make up 43% of the electorate in the US [17]. Since virtually every person begins to suffer some loss of visual acuity after the age of 40 [1], a clear and easy to read and comprehend visual interface should be a design priority. The size and location of menu items on an interface will impact both the speed and accuracy of a user's interaction [23–25]. Font sizes [37] and choice of color [12] are two interface options that should be available to voters. According to [40] legibility, or the typography and layout of the writing on the DRE screen, may increase the speed and accuracy of the voter's interpretation of what is on the screen. Letter spacing, type size, font, lighting, and other environmental factors all play a role in increasing legibility [42].

In short, HCI considerations should be taken into all future design decisions as new DRE technology is rolled out in polling places. Systems that are dynamically controllable, intuitively understood, and give the user options for input, legibility, and typography will be the most successful and accepted by the user.

## 4 Voter Confidence

One of the interesting outcomes of the 2000 presidential race was the outcry over the way voting was handled in the US. When the election between Al Gore and George Bush literally came down to recounted votes in Florida, the country thought it was in a constitutional crisis. Voters did not want to ever have a repeat of the Florida vote. HAVA was the government's response to what happened in Florida, and they hoped that the reforms proposed in the bill would modernize voting. To some extent it did, but by opening the door to doing away with traditional "paper" methods, new problems have arisen. The 2016 election cycle had people asking for paper trails and recounts, but in some cases it was impossible. There are even organizations, such as the Center for Hand-Counted Paper Ballots, whose sole purpose is to lobby for the paper ballot only to be used.

Previous research questions from studies, some posed nearly 20 years ago, regarding the future of e-voting still remain unanswered and are just as valid today. If e-voting systems are found to be problematic, should the results of current and previous electoral match-ups be questioned by the losing party? Should there be a set of national standards and voting machinery that everyone uses, thereby strengthening the process but weakening the decentralized nature of the system? Most of all, if voting irregularities persist with e-voting technologies, can the public's confidence in the electoral process be upheld [18, 42]?

## 5 The Future of e-Voting in the US

By the year 2020, many of the voting systems purchased across the counties and states using HAVA funds from 2002 will have reached their "end of life" and need to be replaced [5].

### 5.1 Emerging e-Voting Technology

In the near term, advancements are being made that could facilitate a number of new developments in how people vote. Los Angeles County, California has the interest and attention of researchers and election officials across the country as it attempts to overhaul its election technology. In contrast to established practice, the county is building its own electronic voting system after years of collecting voter input. Los Angeles election officials hope that by building a system better focused on the needs and preferences of voters, they can spur the voting technology marketplace to offer better solutions at a better value for the voting public. The results of this experiment could be very relevant to other states and localities as they look to replace their increasingly outdated voting technology [38].

Advancements in election technology also have the potential to streamline and simplify the experience of voters in other parts of the voting process, such as obtaining ballot information, registering to vote, verifying voter identity, and travelling to a polling location. Dr. R. Michael Alvarez, co-director of the CalTech/MIT Voting Technology Project, suggests that by 2028, voters will be registered to vote automatically when they obtain a driver's license. In addition, digitized voter rolls could provide streamlined voter identification, and could allow voters to vote at any polling location of their choosing [2].

### 5.2 Internet Based Voting

Looking further into the future, there is increasing pressure around the country to develop a secure, end-to-end verifiable, internet voting system [22]. The U.S. Government spent over a decade and more than 100 million dollars to develop such a system for military service-members stationed overseas. It abandoned this effort in 2014, after federal researchers concluded that mitigating the risks of internet voting was not feasible with current technology [21]. While such a system is still a possibility in the future, continued research and technical advancements will be necessary in areas such as digital protocols, systems engineering, interface design, and system availability and resiliency, among others, in order to make any internet voting system feasible for public elections [11]. The National Institute of Standards and Technology has indicated that it will continue to work with public and private entities in order to resolve these issues [4].

## 6 Conclusion and Research Implications

The future of e-Voting is fairly secure. The US will continue to use various methodologies for e-voting every time there is an election. E-voting will also continue to be used in democracies around the world as technologies continue to evolve.

One thing this study has revealed is the relative lack of academic research on the current e-voting landscape. Most of the research dates back to the middle of the first decade of the 21st century. The next presidential election will take place in the third decade of the 21st century and more current research is warranted. As we reflect on this past presidential election, scholars have both the opportunity and responsibility to offer insight into procedures and technology that will help ensure safe and valid elections.

Research that could bear fruit would be to look into standardizing the election process across all 50 states and county jurisdictions. Currently there is no single standard for all polling sites to follow. Whether or not this would improve or harm the system is ripe for further analysis.

## References

1. Adult Vision: 41 to 60 years of age (n.d.). http://www.aoa.org/patients-and-public/good-vision-throughout-life/adult-vision-19-to-40-years-of-age/adult-vision-41-to-60-years-of-age?sso=y. Accessed 27 Dec 2016
2. Alvarez, R.M.: The future of voting. Wall Street J. (2016). http://www.wsj.com/articles/the-future-of-voting-1478272120
3. Barret, B.: America's electronic voting machines are scarily easy targets, 2 August 2016. https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/
4. Bass, J.: NIST activities on UOCAVA voting, 21 May 2012. https://www.nist.gov/itl/voting/nist-activities-uocava-voting. Accessed 30 Dec 2016
5. Bauer, R.F., Ginsberg, B.L.: The American voting experience: report and recommendations of the presidential commission on election administration. Technical report, pp. 01–112, January 2014. https://www.supportthevoter.gov/files/2014/01/Amer-Voting-Exper-final-draft-01-09-14-508.pdf
6. Bergin, B.: All your lever voting machine questions answered, 21 June 2013. http://www.wnyc.org/story/300838-your-lever-voting-machines-questions-answered-you-have-them-admit-it/?utm_source=sharedUrl&utm_medium=metatag&utm_campaign=sharedUrl. Accessed 21 Dec 2016

7. Bishop, M., Wagner, D.: Risks of e-voting. Commun. ACM **50** (2007). http://escholarship.org/uc/item/3dt089r1
8. Commission, E.: The information society for all (final report). Brussels: IST 2000 Programme (2000). http://ec.europa.eu/smart-regulation/evaluation/search/download.do;jsessionid=g1Uq6EtTNoNIS7pmUYq4B2bmg8ftVJyKnTUNUgHzvAn4F3URMjq2!1168777535?documentId=2820
9. Dayton, R.: Voting Issues: Some Trump Voters Reporting Ballots Switching to Clinton, 8 November 2016. http://pittsburgh.cbslocal.com/2016/11/08/some-problems-reported-as-voters-head-to-polls/
10. Dewey, C.: What was fake on the internet this election: George Soros's voting machines. The Washington Post, 24 October 2016. https://www.washingtonpost.com/news/the-intersect/wp/2016/10/24/what-was-fake-on-the-internet-this-election-george-soross-voting-machines/
11. Dzieduszycka-Suinat, S., Murray, J., Kiniry, J., Zimmerman, D., Wagner, D., Robinson, P., Foltzer, A., Morina, S.: The future of voting: end-to-end verifiable internet voting-specification and feasibility study. US Vote Foundation (2015)
12. Edwards, A.: Computers and people with disabilities. In: Extra-Ordinary Human-Computer Interaction, pp. 19–43. Cambridge University Press, Cambridge (1995). http://dl.acm.org/citation.cfm?id=215601
13. Evans, D., Paul, N.: Election security: perception and reality. IEEE Secur. Privacy Mag. **2** (1), 24–31 (2004)
14. Evans, J.: NAACP gets reports of problems with electronic voting machines in New Hanover County, 25 October 2016. http://www.wbtv.com/story/33467718/naacp-gets-reports-of-problems-with-electronic-voting-machines-in-new-hanover-county. Accessed 26 Dec 2016
15. Fairweather, B., Rogerson, S.: Interfaces for electronic voting: focus group evidence. Electron. Gov. Int. J. **2**(4), 369–383 (2005)
16. Fischer, E.: Election reform and electronic voting systems: analysis of security issues In: CRS Report for Congress No. RL32139. Congressional Research Service, Washington, D.C. (2003). https://epic.org/privacy/voting/crsreport.pdf
17. Fry, R.: Millennials match Baby Boomers as largest generation in U.S. electorate, but will they vote? 16 May 2016. http://www.pewresearch.org/fact-tank/2016/05/16/millennials-match-baby-boomers-as-largest-generation-in-u-s-electorate-but-will-they-vote/
18. Gritzalis, D.A.: Principles and requirements for a secure e-voting system. Comput. Secur. **21** (6), 539–556 (2002). https://doi.org/10.1016/S0167-4048(02)01014-3
19. Hamilton, A., Madison, J., Jay, J., Goldman, L.: The Federalist Papers. OUP Oxford (2008)
20. Henneman, R.L.: Design for usability: process, skills, and tools. Inf. Knowl. Syst. Manag. **1** (2), 133–144 (1999)
21. Internet voting, 4 September 2012. https://www.verifiedvoting.org/resources/internet-voting/
22. Jefferson, D.: If I can shop and bank online, why can't I vote online? 2 November 2011. https://www.verifiedvoting.org/resources/internet-voting/vote-online/
23. Johnson, N., Jones, B.: Is the color of your watch still giving you a fitt? Int. J. Inf. Bus. Manag. **8**(1), 1 (2016)
24. Jones, B.: On-line systems: control button design and characteristic effects on user learning and performance. In: American Conference on Information Systems 2004 Proceedings (2004)
25. Jones, B.M., McCoy, S.: Assessing the Effects of Web-Site Control Design on Single-Step Navigation. University of Pittsburgh, Pittsburgh (2003)
26. Keyssar, A.: The Right to Vote: The Contested History of Democracy in the United States. Basic Books, New York (2009)

27. Kohno, T., Stubblefield, A., Rubin, A.D., Wallach, D.S.: Analysis of an electronic voting system. In: Proceedings of 2004 IEEE Symposium on Security and Privacy, pp. 27–40. IEEE (2004). http://0-ieeexplore.ieee.org.wncln.wncln.org/xpls/abs_all.jsp?arnumber=1301313
28. Kurth, J., Oosting, J.: Records: too many votes in 37% of Detroit's precincts, 13 December 2016. http://www.detroitnews.com/story/news/politics/2016/12/12/records-many-votes-detroits-precincts/95363314/. Accessed 26 Dec 2016
29. Lovgren, S.: Are electronic voting machines reliable? Natl. Geograph. News, 1 November 2004. http://news.nationalgeographic.com/news/2004/11/1101_041101_election_voting.html
30. McDonald, F.: The Presidency of George Washington. University Press of Kansas, Lawrence (1974)
31. McKeever, J.: High turnout, long lines as people of Connecticut cast their votes, 8 November 2016. http://fox61.com/2016/11/08/connectictut-voters-cast-their-votes/
32. Mechanical Lever Machines (n.d.). http://www.fec.gov/pages/lever.htm. Accessed 21 Dec 2016
33. Mello-Stark, S.: Some states—including swing states—have flawed voting systems, 1 November 2016. http://www.vox.com/the-big-idea/2016/11/1/13486386/election-rigged-paper-trail-audit. Accessed 26 Dec 2016
34. Meyers, S.: The most important design guideline. IEEE Softw. **21**(4), 14–16 (2004)
35. Moeller, P.: Technology still a big disconnect for older Americans, 27 February 2012. http://money.usnews.com/money/blogs/the-best-life/2012/02/27/technology-still-a-big-disconnect-for-older-americans. Accessed 27 Dec 2016
36. Morris, G., Scott, R., Woodward, A.: Polls Apart: A Future for Accessible Democracy (Electoral Commission). SCOPE, London (2002)
37. Nielsen, J.: Let users control font size. Jakob Nielsen's Alertbox, 19 August 2002
38. Norden, L., Famighetti, C.: America's voting technology crisis. The Atlantic, 15 September 2015. http://www.theatlantic.com/politics/archive/2015/09/americas-voting-technology-crisis/405262/
39. Preece, J., Rogers, Y., Sharp, H.: Interaction Design: Beyond Human-Computer Interaction. Wiley, New York (2002). https://www.mysciencework.com/publication/show/fbabc4fca2d1da90150213ad37561404
40. Reynolds, L.: The legibility of printed scientific and technical information. In: Easterby, R., Zwaga, H. (eds.) Information Design. Wiley, Chichester (1984)
41. Riley, M., Robertson, J., Kocieniewski, D.: The computer voting revolution is already crappy, buggy, and obsolete. Bloomberg.com, 29 September 2016. https://www.bloomberg.com/features/2016-voting-technology/
42. Roth, S.K.: Disenfranchised by design: voting systems and the election process. Inf. Des. J. **9** (1), 29–38 (1998)
43. Simons, B.B.: Electronic voting systems: the good, the bad, and the stupid. ACM Queue **2** (7), 20–26 (2004)
44. Torres, K.: Georgia early voting machine suspected of "changing" votes, 27 October 2016. http://www.ajc.com/news/state–regional-govt–politics/georgia-voting-machine-suspected-flipping-presidential-votes/woKEUgpDDEyaw9o4J318XJ/. Accessed 26 Dec 2016
45. Voting Equipment in the United States (n.d.). https://www.verifiedvoting.org/resources/voting-equipment/

46. Voting methods and equipment by state (n.d.). https://ballotpedia.org/Voting_methods_and_equipment_by_state. Accessed 21 Dec 2016
47. Wand, J.N., Shotts, K.W., Sekhon, J.S., Mebane Jr., W.R., Herron, M.C., Brady, H.E.: The butterfly did it: the aberrant vote for Buchanan in Palm Beach County, Florida. Am. Polit. Sci. Rev. 793–810 (2001)
48. Wertheimer, M.: Trusted agent report: diebold AccuVote-TS voting system. Prepared by: RABA Innovative Solution Cell (RiSC), 20 January 2004