USENIX Journal of Election Technology and Systems (JETS)
Volume 2, Number 3 • July 2014
www.usenix.org/jets/issues/0203

Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II

Claudia Z. Acemyan[1], Philip Kortum[1], Michael D. Byrne[1, 2], Dan S. Wallach[2]
[1]Department of Psychology, Rice University
[2]Department of Computer Science, Rice University
6100 Main Street, MS-25
Houston, TX 77005 USA
{claudiaz, pkortum, byrne}@rice.edu and dwallach@cs.rice.edu

ABSTRACT
In response to voting security concerns, security researchers have developed tamper-resistant, voter verifiable voting methods. These end-to-end voting systems are unique because they give voters the option to both verify the system is working properly and to check that their votes have been recorded after leaving the polling place. While these methods solve many of the security problems surrounding voting with traditional methods, the systems' added complexity might adversely impact their usability. This paper presents an experiment assessing the usability of Helios, Prêt à Voter, and Scantegrity II. Overall, the tested systems were exceptionally difficult to use. Data revealed that success rates of voters casting ballots on these systems were extraordinarily low. Specifically, only 58% of ballots were successfully cast across all three systems. There were reliable differences in voting completion times across the three methods, and these times were much slower than previously tested voting technologies. Subjective usability ratings differed across the systems, with satisfaction being generally low, but highest for Helios. Vote verification completion rates were even lower than those for vote casting. There were no reliable differences in ballot verification times across the three methods, but there were differences in satisfaction levels, with satisfaction being lowest for Helios. These usability findings—especially the extremely low vote casting completion rates—highlight that it is not enough for a system to be secure; every system must also be usable.

INTRODUCTION
For centuries there has been a desire for auditability in elections. In mid-19th century America, groups of voters stood in public venues and called out their ballot choices to the election clerks, while a judge tallied the votes (Jones, 2001). The advantage of this voting method was that anyone could listen to the vocal expression of preferences and keep their own vote count, which prevented practices like ballot box stuffing. While this oral voting method may have increased the accuracy of vote counting, voters' desire for privacy was not addressed, enabling bribery and coercion. In response, during the late 1800s, voting jurisdictions began to introduce the use of the secret, Australian ballots that listed all the candidates for the same office on the same sheet of paper (which was issued to voters at the polling station) and guaranteed voters privacy in preparing ballots inside a booth (Brent, 2006). This voting system ensured that voters prepared their own ballot expressing their intent while preserving anonymity. Yet this voting method was not perfect; there was not a means to audit the election—leaving a long-standing tension between auditability and privacy in elections.

e2e Voting Systems

So that cast ballots can be both auditable and anonymous, which would ultimately improve the integrity of elections, voting security researchers have developed secure, voter verifiable systems, also known as end-to-end (e2e) voting systems (e.g., Adida, 2008; Carback et al., 2010; Chaum et al., 2010; Clarkson, 2008; Ryan et al., 2009). e2e systems are voting methods that aim for ballots to be cast as voters intend and counted as cast. To make sure these systems are functioning as they should, they are designed so that both voters and observers can audit, or verify, various aspects of the voting method—all while preserving voter privacy.

How do these e2e systems work? To protect votes from malicious attacks, cryptographic protocols and auditing mechanisms are used. The cryptographic methods make it very difficult to undetectably attack and/or alter the e2e systems so that election outcomes would be impacted. Then, with the ability for voters and observers to audit the system, people are given a means to make sure the system is working as it should—from making certain that intended selections are the actual votes cast to checking that the ballots are accurately counted, resulting in a fair, accurate election. In order to protect the identity and preferences of the voter, information that could identify the voter is never associated with the ballot. Instead, e2e systems use a unique ballot identifier (such as a code associated with each ballot), allowing a voter to find and identify their own ballot while preventing others from being able to tell that the specific ballot belongs to that individual. In addition, when a voter goes through the verification process to check that their ballot was cast and recorded, their actual ballot selections are never revealed. Rather, the voter may be shown another type of information that confirms that their ballot selections are recorded without disclosing the actual selections.

Examples of e2e voting systems include Helios (Adida, 2008), Prêt à Voter (Ryan et al., 2009), and Scantegrity II (Chaum et al., 2008). These three systems have been selected to be representative examples of voter verifiable systems for several reasons. First, they are largely accepted and discussed as secure voting methods within the voting research community. Furthermore, they represent a spectrum of the different solution types that have been proposed for use in polling stations (it has been suggested that Helios can be modified and adapted for use at polling sites in order to prevent coercion). Helios is a web-based system and an exemplar of Benaloh-style schemes (Benaloh, 2006). Prêt à Voter (PaV) is a simple, novel, paper-based scheme with many variants that are being considered for use in various elections all over the world. Scantegrity II is another paper-based scheme that incorporates the traditional paper bubble ballot. All three voting systems have been used, or will be used, in actual elections: Helios was used in the presidential election at the Universite Catholique de Louvain, Belgium (Adida et al., 2009), International Association for Cryptologic Research's board of directors election (IACR, n.d.), and Princeton Undergraduate Elections (see princeton.heliosvoting.org). PaV has been used in student elections in both Luxembourg and Surrey (P. Ryan, personal communication, April 3, 2014), and it will be used in the November 2014 Victorian State elections (Burton et al., 2012). Scantegrity II was used in the November 2009 municipal election in Takoma Park, Maryland (Carback et al., 2010).

Helios

Helios is a web-based, open-audit voting system (Adida, 2008; Adida et al., 2009) utilizing peer-reviewed cryptographic techniques. From a security standpoint, system highlights include browser-based encryption, homomorphic tallying, distributed decryption across multiple trustees, user authentication by email address, election-specific passwords, and vote casting assurance through various levels of auditing.

From the voter's standpoint, Helios appears to be similar to direct recording electronic voting systems (DREs) like VoteBox (Sandler, et al, 2008). Instances of the user interface can be seen in Appendix 1. The following outlines the vote casting process from the voter's perspective (the exact steps have the potential to vary from voter to voter, hence the following are potential procedures): 1) The voter logs into their email account to obtain the election's website address (this information can also be disseminated through other methods). 2) After navigating to the election's Helios Voting Booth webpage, the voter reads through the voting system instructions and clicks "start" to begin voting. 3) The voter completes the ballot one race at a time by checking the box next to the desired candidate or proposition and then clicking next/proceed to move onto the next screen. 4) The voter reviews his or her ballot and then clicks the "confirm choices and encrypt ballot" button. 5) The voter records his or her smart ballot tracker by printing it out and proceeds to submission. 6) The voter logs in with their email address to verify their eligibility to vote. 7) The voter casts the ballot associated with their smart ballot tracker. 8) The voter views a screen indicating their vote has been successfully cast.

For a voter to verify their vote, or check that it was in fact cast in the election, the following sequence is typical: 1) In the user's inbox, open and view an email from the Helios Voting Administrator. The e-mail indicates that their vote has been successfully cast and displays a link where the ballot is archived. 2) The voter clicks on the ballot archive link. 3) The voter views a screen that says "Cast Vote" along with their smart ballot tracker. The voter clicks on details and views the code associated with the ballot, which can be used on an auditing page to verify that their ballot is encrypted correctly. 4) The voter returns to the election home page and clicks on "Votes and Ballots." 5) The voter observes on the Voter and Ballot Tracking Center page that their smart ballot tracker is shown within the list of cast votes.

Prêt à Voter

The next system, Prêt à Voter (PaV), inspired by Chaum's (2004) visual cryptographic scheme, is a voting system that allows voters to vote with paper forms (with randomly ordered races and selections for each race), which can be physically modified to then serve as an encrypted ballot. This voting method is auditable at numerous phases by both voters and teams of auditors (Ryan et al., 2009). The system is flexible in that it allows different encryption schemes and cryptographic mechanisms to be used as needed.

PaV was intended to provide voters with a simple, familiar voter experience. Images of this study's voting instructions, ballot, receipt, and vote verification pages can be found in Appendix 2.

To vote with the PaV system, the voter follows these typical steps: 1) A sealed envelope enclosing a paper ballot is given to the voter. The voter opens the envelope and finds an instruction sheet and cards that make up the ballot. 2) To mark their selections on the ballot cards, a cross (x) is marked in the right hand box next to the name of the candidate or proposition that the voter wants to select. 3) After completing the ballot, the voter detaches the candidates lists from their selections or marks. 4) The candidates lists are shredded. 5) The voter walks over to the vote casting station and feeds the voting slips into the scanner. 6) The voting slips are placed in the ballot box. 7) The voter takes a printed receipt, which shows images of the scanned voting slips along with the website and ballot verification code needed to confirm that they voted.

For a voter to verify their vote using PaV, the voter might typically perform the following sequence on a computer or mobile device: 1) Navigate to the election verification website, which is printed on their receipt. 2) Enter the ballot verification code on the home page and submit it. 3) View the vote validation page that confirms the entered verification code is valid. This page also

displays images of every ballot card—thereby displaying every selection on every card (without any candidates lists) that makes up their ballot.

Scantegrity II
The third method, Scantegrity II, is an optical scan voting system that enables a voter to vote with a paper bubble ballot, enhanced by traceable confirmation codes that can be revealed by invisible ink decoder pens (Chaum et al., 2008). This voting system can be audited by voters or any other interested party.

Scantegrity II was developed so that voters could still use a familiar voting technology—an optical scan bubble ballot that they already have experience using. Images of the paper bubble ballot and other voting system materials used in this study can be found in Appendix 3.

To cast a vote using the Scantegrity II voting method, a voter would typically do the following: 1) Read the instructions on both the ballot and separate vote verification sheet. 2) Use the special marking device to make ballot selections—and consequently reveal codes—by filling in the appropriate bubbles. 3) Record on the separate vote verification sheet the revealed confirmation codes found inside each marked bubble. Also record on this sheet the ballot ID / online verification number that is found on the bottom right corner of the ballot. 4) Walk over to the ballot casting station to scan in the ballot and have it then placed in the ballot box. 5) Hand the vote verification sheet to the polling station official so that they can stamp "Cast Ballot" on it. 6) Choose whether or not to keep their verification sheet.

To verify the votes, a voter may perform the following sequence at their home or office: 1) Navigate to the election's vote verification web page. 2) Enter their unique online verification number associated with their ballot. 3) View a confirmation webpage that says the ballot has been cast and processed. This page also displays the online validation code along with a list of the voter's confirmation codes, with each code corresponding to a ballot selection.

Understanding the Usability of e2e Voting Systems
As can be seen from the vote casting and vote verification procedures, the three e2e systems are complex from the standpoint of the voter. Many of the processes required to use the systems are both long and novel in the context of voting. This is of concern because voters already have difficulty voting with standard paper ballots due to design deficiencies like insufficient instructions and confusing ballot designs (Norden et al., 2008). If additional e2e mechanisms are then laid on top of these problems, this raised the question of whether or not voters' abilities to cast their votes will be further degraded. If people cannot use the system to vote, then voters will likely be disenfranchised and election outcomes might be changed—tremendous threats to democracy. Furthermore, if people are not able to verify that their ballot has been cast because the system is too hard to use, then the system is not auditable—leaving room for inaccuracy and corruption. Consequently, voting researchers need to understand the usability of each system and how it compares to other voting technologies.

System usability is defined as the capability of a range of users to be able to easily and effectively fulfill a specified range of tasks within specified environmental scenarios (Shackel, 1991). In the context of voting, usability might be thought of as whether or not voters can use a voting method to successfully cast their votes. Per ISO standard 9241-11 (1998), there are three suggested measurements of usability: effectiveness, efficiency and satisfaction. As established in previous voting usability research (Byrne et al., 2007; Laskowski et al., 2004), effectiveness addresses whether or not voters are able to select, without error, the candidate or proposition for which they

intend to vote. One way to measure effectiveness is by calculating error rates. Efficiency concerns the amount of resources required of a voter to attempt achieving his or her goal. This variable can be measured by calculating task completion times, or the amount of time it takes to vote or verify a vote. The third measure, satisfaction, is defined as the voter's subjective perceptions of a voting system after using it—such as how hard or easy it is to vote using the method. Satisfaction can be measured with a standardized instrument like the System Usability Scale, or SUS (Brooke, 1996).

The only way to know if e2e systems are usable is to empirically test them. While other studies have reported on the usability of select e2e systems (Carback et al., 2010; Karayumak, 2011; Weber et al., 2009, Winckler et al., 2009), none have experimentally evaluated the voting methods along all three suggested measurements outlined by both ISO standard 9241-11 and the 2004 NIST report on voting system usability (Laskowski et al., 2004).

To address this lacuna, this study tested the usability of the three e2e voting systems presented above: Helios, Prêt à Voter, and Scantegrity II. When applicable, the same materials and protocols were used from the previous voting studies conducted by Rice University's human factors voting laboratories (e.g., Byrne et al., 2007; Campbell et al., 2009; Campbell et al., 2011; Everett, 2007; Everett et al., 2008; Holmes & Kortum, 2013) to allow for comparison of usability findings across different voting technologies. The goals of this research project were to understand whether voters can use these e2e voting methods to cast and verify their votes, identify system attributes that might be preventing voters from fulfilling their goals of vote casting and verifying, and help us to make recommendations that might enhance the design and implementation of e2e systems.

METHODS

Participants

Thirty-seven participants who were U.S. citizens and 18 years or older (the minimum age to vote in the U.S.) were recruited through an online advertisement in Houston, Texas. They were paid $40 for participating in the study. The mean age was 37.1 years, with a median of 35 and a range of 21 to 64. There were 22 male and 15 female participants. Participants were African American (14, 38%), Caucasian (10, 27%), Mexican American / Chicano (4, 11%), Hispanic / Latino (4, 11%), and other ethnicities (5, 13%). As for the participants' educational background, 2 (5%) had completed high school or the GED, 23 (62%) completed some college or an associate's degree, 8 (22%) were awarded a bachelor's degree or equivalent, and 4 (11%) held a post-graduate degree. English was the native language of 36 of these participants. All had self-reported normal or corrected-to-normal vision. Participants rated their computer expertise on a scale from 1 to 10, with one being novice and 10 being expert; the mean was 8.2 with a range of 5 to 10. 33 participants had voted in at least one national election, with an average of 3.8 and a range of 0 to 21. Participants had, on average, voted in 5.1 state and local elections. This is a diverse and representative sample of real voters.

Design

A within-subjects design was used, in which every participant used three different voting methods. The within-subjects study design increased the statistical power of the analysis such that the sample size of 37 was more than adequate to detect even small effects. The three voting systems used in this experiment were Helios, Prêt à Voter, and Scantegrity II. Each participant voted with all three methods. All possible orders of presentation were used, and subjects were randomly assigned an order.

So that voters knew for whom they should vote, they were given a list of candidates and propositions. Their list was either primarily Republican and contained 85% Republican candidates, or it was primarily Democratic with 85% being Democratic candidates. Both lists had "yes" votes for four propositions and "no" votes for two. These two lists were the same as those used in our previous studies. Participants were randomly assigned one of the two slates.

Per the ISO 9241-11 definition of usability (ISO, 1998), there were three main dependent variables: errors (effectiveness), completion time (efficiency), and subjective usability (satisfaction). Three types of errors were included in the effectiveness measure. First, we measured the inability to either cast a ballot and/or later verify votes. For example, if a participant completed a ballot but never cast it by scanning it, then this was counted as an error with PaV and Scantegrity II. In Helios, if a voter encrypted his or her ballot but never continued on to verify their eligibility to vote (by logging in with their email account)—an action that is required at this point in the voting process in order to move onto the actual vote casting step, then this would be counted as a failure to cast. Second, we recorded per-race errors, which are defined as deviations on the voter's ballots from the list of candidates and propositions given to the voter, which they were instructed to select. A per-contest error rate for each ballot was computed for every participant. Third, overall ballot errors were measured. Overall ballot errors are defined as a ballot with at least one deviation from the list of candidates and propositions given to the voter. For example, whether a voter selected one wrong candidate or ten wrong candidates, the ballot would be classified as having errors on it.

To measure efficiency, voting and verification completion times were used. Both voting and vote verification times were measured with a stopwatch. The stopwatch was started after the experimenter said the participant could begin, and it was stopped when the participant indicated that they were finished with their task.

The System Usability Scale was used to measure satisfaction. The SUS contains ten subscales. Each subscale is a 5-point Likert scale that measures an aspect of usability. The ratings for each subscale are combined to yield a single usability score ranging from 0 to 100, with lower scores being associated with lower subjective usability.

Data were also collected on other factors such as technologies used to vote in previous elections, computer experience, perceptions of voting security, and preferred voting technology.

For each e2e system, the dependent measures described above were collected for both the vote casting portion of the system (i.e., the procedures the voter must go through in order to make their selections on a ballot and successfully cast the ballot), as well as the vote verification portion of the system (i.e., the procedures required of the voter to be able to check that their votes were cast and included in the final election tally). The two portions of the system were examined separately since vote verification is an optional procedure not required to cast a ballot and have it be counted. This study did not explore the usability of the optional auditing processes associated with the systems.

Procedures

The study began with participants giving their informed consent. They were then read instructions for the experiment. Subjects were instructed to vote on all three ballots according to their list of candidates and propositions. Because verification is neither currently an option in U.S. elections, nor required to cast a vote with e2e systems, voters were specifically told that they would be asked

to verify their vote at the end of the voting process, and that they should take whatever steps were necessary to insure that they could perform this verification step. Participants then voted with one of the three voting methods (order was counterbalanced across participants, all orders used), each in its own room to prevent confusion as to which equipment was associated with each voting system. After voting on a system, the participants immediately completed the System Usability Scale. When completing the instrument, participants were specifically instructed to evaluate the *voting* system they had just used. Next, participants verified their vote using the same system and completed another SUS, being explicitly instructed to evaluate only the *verification* system they just used. They then went through this process for the remaining two systems. At the end of the experiment, participants completed a final survey packet that was composed of 49 questions. The survey covered topics like demographics, computer expertise, previous voting experience, security, voting method comparisons, voting method instructions, and vote verification. Last, participants were debriefed, compensated, and thanked for their time.

We used the modified form of the System Usability Scale as presented in Bangor et al. (2008) to assess subjective usability or satisfaction. In this version of the SUS, the word "cumbersome" is replaced with "awkward." We also replaced the word "system" with the words "voting system" or "voting method," and "verification system" or "verification method" as appropriate. We made this particular change based on user feedback from our pilot study's subjects. Altering the SUS in this way has been shown to have no impact on the scale's reliability (Sauro, 2011).

It should be noted that the participants' desktops were mirrored to a monitor that only the experimenter could view in another part of the room. Mirroring the monitors was intended to aid the experimenter in observing the participant's actions in an unobtrusive fashion. Mirrored monitors also allowed the experimenter to score the errors on Helios' ballot in real time and determine if voters verified their votes across all three systems.

Materials

For all three systems, the following hardware was used: The computers were Dell Optiplex desktops with 17" monitors. The scanners were VuPoint Solution Magic Wands; these scanners were selected because they would automatically feed and scan sheets of paper inserted by the user. The shredders used were Amazon Basics 8 or 12-sheet automatic shredders. The printers used were the HP Deskjet 1000 (Helios) and the HP LaserJet Pro Laser Printer (PaV), both of which are single function printers. All computers had Windows XP operating systems and Google Chrome version 32 as the default web browser. This web browser was selected because it was compatible with all voting and verification systems tested in this study. The only icons on the computers' desktops were the hard drive, trashcan, and Google Chrome.

Candidates and propositions on the ballots were those used in our previous experiments (e.g., Byrne et al., 2007; Everett et al., 2008). The candidates' names had been randomly generated through online software. The ballot was comprised of 21 races, which included both national and county contests, and six propositions. The length and composition of the ballot was originally designed to reflect the national average number of races. The format and layout of each system's ballot followed the criteria outlined by the system developers in published papers.

The Helios voting system and election was set up and run through Helios' website at vote.heliosvoting.org during the winter of 2013-2014. A Gmail login provided to the participant was used to obtain Helios voting instructions, access the election link, confirm eligibility/identity before casting the ballot, and/or view the confirmation email sent after ballot casting. See Appendix 1 for the study materials used in association with this voting system.

Since PaV had not been previously developed to be used in an election with numerous races (as is the case in the United States), our team developed the system based on published papers about PaV (e.g., Lundin & Ryan, 2008; Ryan et al., 2009; Ryan & Peacock, 2010; Ryan & Schneider, 2006), the PaV website (Prêt à Voter, n.d.), and in consultation with Peter Ryan, who first created the system. It should be noted that the security mechanisms were not implemented in the system. Nevertheless, from the voter's perspective, the system appeared to operate as a fully functional, secure system. See Appendix 2 for system materials.

This study's implementation of Scantegrity II was heavily based on materials used in the 2009 Takoma Park, Maryland election, in which voters used the system to elect the mayor and city council members (Carback et al., 2010). We also referred to published articles about the system and corresponded through email with Aleks Essex, a researcher who has direct experience with the implementation. When aspects of the system that might have potential to impact usability were not specified, best practices in human factors were followed. Also, when possible, every effort was made to keep system properties (such as font) constant across systems. Like PaV, this system was not a fully functional prototype from a security perspective. Instead, it appeared to be fully functional from the voter's perspective. See Appendix 3 for Scantegrity II's materials.

RESULTS

There were no differences in the findings based on whether participants were told to vote for mostly Republicans or mostly Democrats according to their directed voting list, so we treated this as a single condition. There were also no differences in the efficiency, effectiveness, and satisfaction findings based on whether or not participants were able to cast a vote or later verify a vote. This was also treated as one condition. The analysis was a repeated measures ANOVA unless otherwise specified. *p*-values were adjusted by Greenhouse-Geisser (G-G) correction when appropriate. FDR adjustments to post-hoc tests were performed when necessary.

Vote Casting

Effectiveness

Figure 1 shows the number of voters who thought they cast a vote with each system versus the number of actual cast votes. As can be seen, a reliably higher percentage of voters *thought* they had cast a vote that would be counted in election totals than the percentage of ballots that they *actually* cast, (tested with binomial linear mixed model, $z = 4.42$, $p < .001$). The interaction between these two variables across voting systems was not reliable. These completion rate findings are extremely troubling. If the tested e2e voting systems are used in a real election, on a large scale, high percentages of voters might not be able to vote—resulting in disastrous outcomes. These failure-to-cast findings are especially unacceptable when many of the other systems tested in our lab produced 100% ballot casting completion rates (e.g., Byrne et al., 2007).

Per-contest error rates as a function of system can be seen in Figure 2. There was no reliable evidence for an effect of system type on these errors, $F(1.1, 40.9) = 2.70$, $MSE = 0.00$, $p = .104$, $\eta^2 = .09$. In this regard, e2e systems seem to be performing better than previously tested voting systems that had error rates ranging from less than 0.5% to about 3.5% (Byrne et al., 2007). With that being said, this potential advantage over other voting technologies is moot if voters cannot cast votes at reasonable rates.

Table 1 shows the frequency of error-containing ballots by voting system. Overall, 5 of the 111 (5%) ballots collected contained at least one error. Again, this error rate is lower than those previously reported (see Byrne et al., 2007). Based on both the per-contest error rates and error

rates by ballot, voters using e2e systems make few errors selecting candidates and propositions on their ballots.

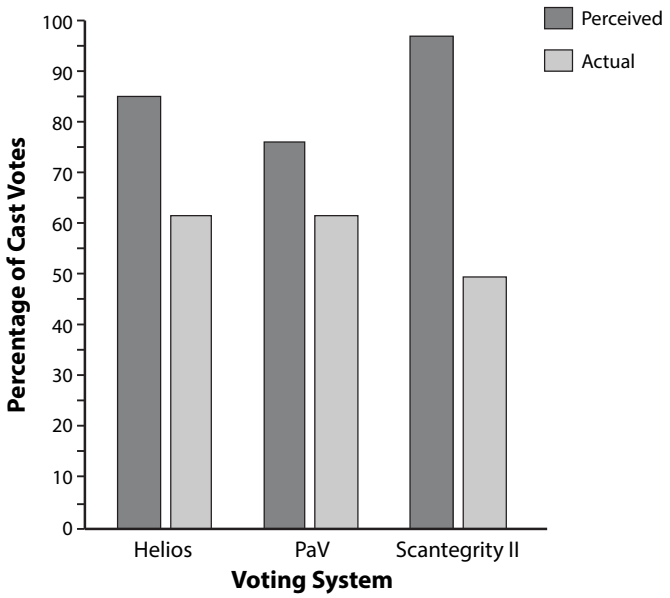


Figure 1. Percentage of cast ballots as a function of voting system, with different colored bars representing perceived and actual cast votes

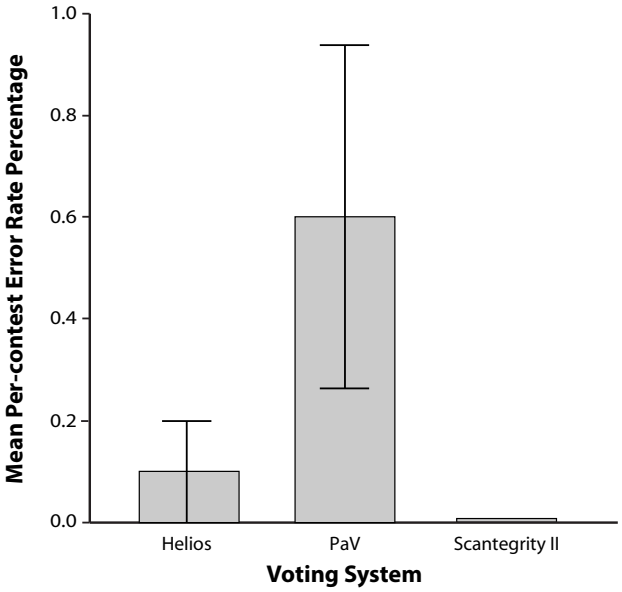


Figure 2. Mean per-contest error rate percentage as a function of voting system type, with error bars depicting the standard error of the mean

Table 1. The number and percent of ballots with one or more errors as a function of voting system type

	Helios	PaV	Scantegrity II
Number of Ballots with Errors	1 (3%)	4 (11%)	0 (0%)

Efficiency
Average ballot completion time as a function of voting system is presented in Figure 3. As can be seen, there are differences in voting times across the systems, $F(2, 72) = 8.45$, $MSE = 34{,}457$, $p = .001$, $\eta^2 = .23$. Pairwise tests revealed all three means were reliably different. Participants took the least amount of time to vote with Helios and the most amount of time to vote with Scantegrity II. In prior research, ballot completion time is generally not sensitive to voting technology. Average completion time for the identical ballot using arrow ballot, bubble ballot, punch card, and lever machine voting methods is approximately 231 seconds (Byrne et al., 2007) and 290 seconds across sequential DRE, direct DRE, bubble ballot, lever machine, and punch card systems (Everett et al., 2008). Thus, the e2e systems impose a substantial time cost on voters.

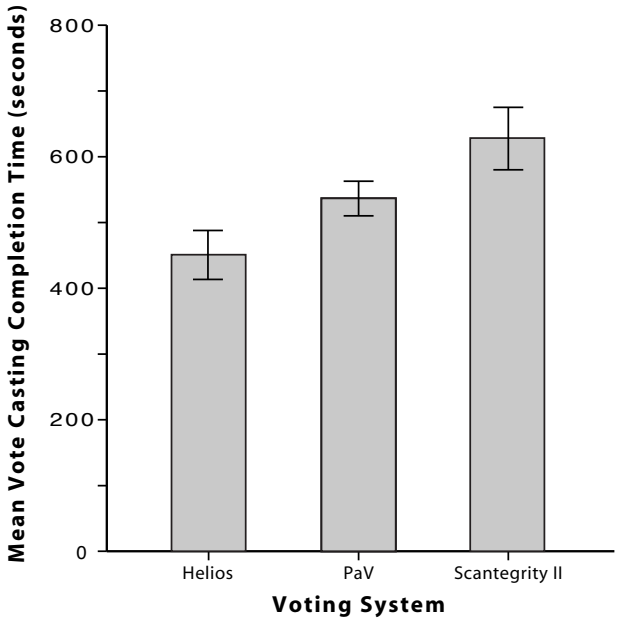


Figure 3. Mean vote casting completion time as a function of voting system, with error bars depicting the standard error of the mean

Satisfaction
As can be seen in Figure 4, SUS ratings (out of 100 possible points) differ across the three e2e voting systems, $F(2, 72) = 5.28$, $MSE = 624$, $p = .007$, $\eta^2 = .13$. Pairwise *t*-tests revealed that participants were reliably more satisfied with the usability of Helios, but there was not a statistically reliable difference in satisfaction ratings between PaV and Scantegrity II. When compared to previously tested voting methods, these SUS scores are comparable or lower than those previously seen (Byrne et al., 2007). Using the assessment of fitness for use scale (based on

the SUS score) proposed by Bangor, Kortum and Miller (2009), Helios would be judged as "acceptable," while PaV and Scantegrity II would be on the low end of "marginal acceptability." Based on all of these SUS findings, voters' satisfaction with using Helios was relatively good, but their satisfaction with using the other two systems was between poor and good—suggesting that there is room for improvement in future system iterations.

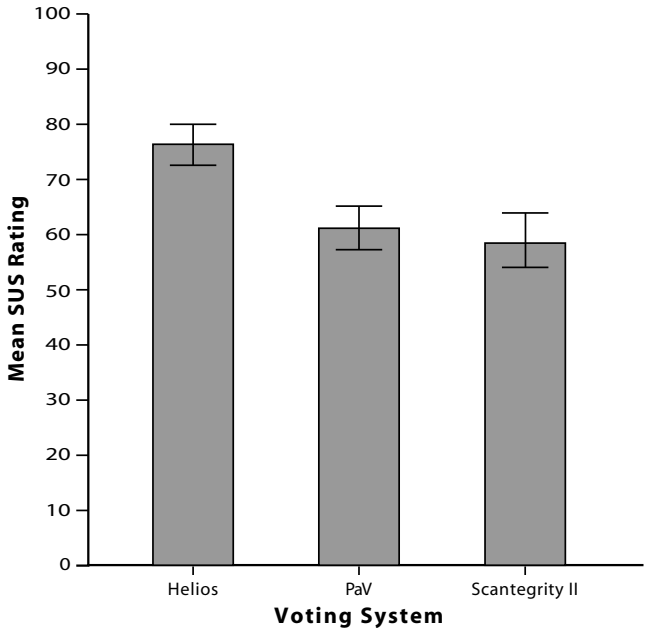


Figure 4. Mean SUS rating as a function of voting system, with error bars depicting the standard error of the mean

Vote Verification

Effectiveness

Figure 5 shows the number of participants who were able to actually verify their vote through any means versus those who thought they verified as a function of system type. There was no reliable effect of system or difference between perceived versus actual completion rates. However, these vote verification task completion rates are lower than those for vote casting (again, tested via binomial linear mixed model, $z = 2.17$, $p = .030$).

With Helios, 16 (43%) voters performed any type of vote verification action. Of these, only 8 (50%) recorded their smart ballot tracker, which allows them to identify their particular vote in the online vote center. Two of the 16 participants verified by viewing the verification email sent to them after voting. The rest of the subjects verified by viewing their information on the Helios election website, keeping in mind that many did not have a recorded smart ballot tracker to which they could refer. With Scantegrity II, 14 (38%) voters performed some type of vote verification. Of these, only nine attempted to record all 27 vote verification codes; only a *single* person wrote down all 27 correctly. Based on these results, for both Helios and Scantegrity II participants engaged in a wide range of behaviors when they tried to check that their vote was cast in the mock elections. PaV was designed so that the verification output required to check on the ballot was automatically given to voters upon casting their ballots, and there was only one way in which they

could check on their ballots, so more specific findings on verification actions are not reported for the system.

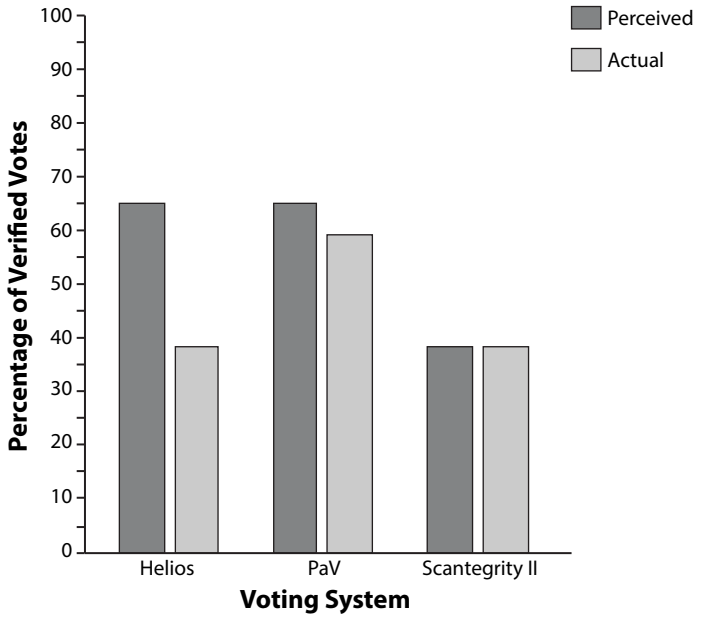


Figure 5. Percentage of verified votes as a function of voting system, with different colored bars representing perceived and actual verified votes

Efficiency

Results for vote verification time as a function of voting system are presented in Figure 6. The effect of voting system was suggestive but not statistically reliable, $F(1.2, 7.2) = 3.74$, $MSE = 21{,}559$, $p = .089$, $\eta^2 = .38$. It should be noted that the amount of time it takes someone to *verify* their vote with these e2e voting systems is similar to the amount of time it takes to *vote* on previously tested voting technologies (Byrne et al., 2007).

Satisfaction

Figure 7 depicts the mean SUS score as a function of system type. The effect of voting system was reliable, $F(2, 12) = 7.86$, $MSE = 792$, $p = .007$, $\eta^2 = .57$. Pairwise *t*-tests indicated that Helios was rated lower than PaV on the subjective usability measure; there was not any evidence to support other statistically reliable differences. Using the assessment of fitness for use scale (Bangor et al., 2009), Helios would be judged as being "not acceptable," Scantegrity II would be on the high end of "marginal," and PaV would be classified as "good." To summarize these findings, Helios' verification system had a staggeringly low subjective usability rating, emphasizing how bad participants thought of the system's usability. Participants did rate PaV higher (that is, that they thought PaV was easier to use).

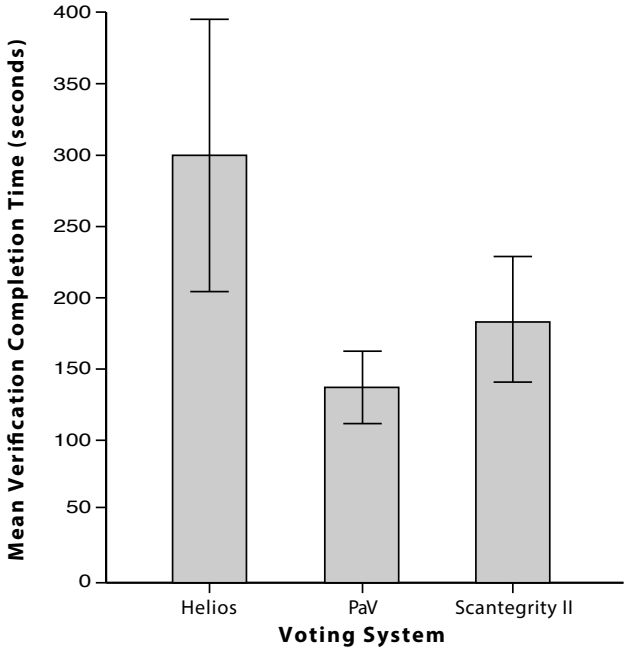


Figure 6. Mean verification completion time as a function of voting system, with error bars depicting the standard error of the mean

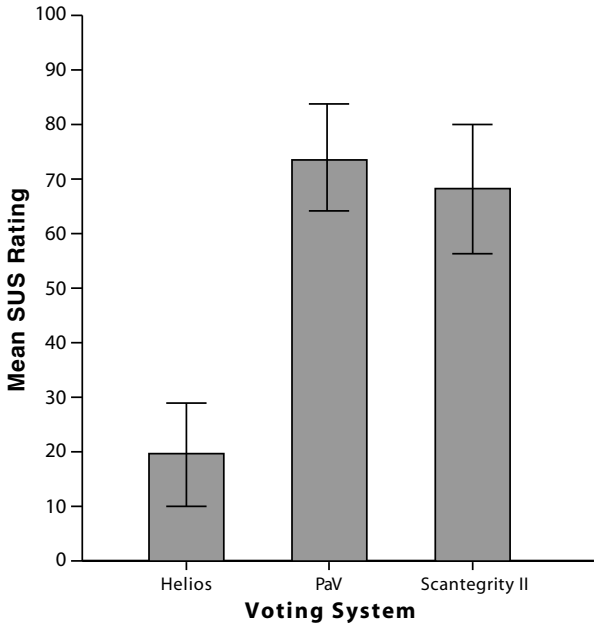


Figure 7. Mean SUS rating for the vote verification process as a function of voting system, with error bars representing the standard error of the mean

DISCUSSION

Generally, all of the tested e2e voting systems appear to have momentous usability issues based just on the high failure-to-cast rates. Perhaps more troubling, however, is the fact that many of the participants in this study *thought* they cast a vote, but actually did not. These findings would have huge implications in a real election. Since they believe they did in fact vote, they would not even know to tell someone that they could not cast a vote to receive assistance or notify officials that there might be usability problems. As for the voters who recognize they cannot vote, they might seek help or they might give up. Even if they are able to eventually cast a vote after receiving direction, they might choose not to vote in the future, and thus the e2e systems would disenfranchise voters.

The low success rates observed in the vote verification part of the systems are also troublesome. If voters cannot check on their ballot after voting, then fewer people will be able to check that the system is working properly. The voter might also have lower confidence in the system since they know the verification feature is available, but they were not able to use it for some reason. Even if a voter is able to verify that his or her vote was cast, it might lead to frustration levels that are associated with future system avoidance, meaning—again—there will be fewer people to check on the integrity of the system. One potentially unintended consequence of these verification systems is that it adds another opportunity for errors to be committed. If the voters write down their verification information incorrectly (a smart ballot tracker in the case of Helios or a selection's confirmation code with Scantegrity II) then they might think their vote was lost, thrown out, or not recorded correctly. If the voter then reports to an election official that something is wrong, a new set of serious problems emerge: election officials and voters might think the election results are incorrect, when in fact they are correct. If widespread, this kind of simple and foreseeable failure could lead to a general lack of confidence in the results among the "average" voter who tried to verify their vote, but failed. These are all serious ramifications—highlighting that it is not enough for a system to be secure. Every system must also be usable.

Why are these systems failing?

It is clear that while the e2e mechanisms may significantly enhance the security of these voting systems, the enhancements come at the cost of usability. The additional and unfamiliar procedures impact the very essence of the voting process—the ability to cast a vote—and do so in ways that cause many users to not even be aware that they have failed. We believe that there are several general design choices that led to the results reported here, yet each of these can be overcome with design modifications and additional research efforts.

1) Security Isn't Invisible

All of the tested e2e voting systems function in a way that require users to be an active part of the security process. These additional steps likely lead to increased cognitive load for the user, and that increased load can lead to failures. In contrast, an ideal security mechanism requires no such additional effort on the part of the user. In novice parlance, "it just happens." The user is neither required to take action nor even know that there is enhanced security implemented on his behalf. For example, banks encrypt their web-based transactions, but the user does not take part in enabling or executing these additional safety measures.

2) Tested e2e Systems Do Not Model Current Systems to the Greatest Degree Possible

Many of the observed usability difficulties in this study can likely be attributed to designs that work differently than users expect. Many participants were experienced with voting and had seen previous (albeit, different) implementations of what a voting system "should" look like and how it

"should" behave. For the most part, the tested e2e systems deviated from these expectations significantly, leaving users confused. In this confusion, participants might have recalled their previous experience with voting systems, and then used that to guide their interactions. Since their previously used voting systems do not work in the same way as e2e voting systems, referring to previous experience inevitably led to decreases in performance and the commission of errors where the users' prior voting model and the system's actual function did not match. This may explain why Helios had higher SUS ratings than PaV and Scantegrity II. Many participants verbally expressed that they liked using the computer to vote since they already use them daily—in other words, they got to use a platform with which they were familiar. Of the three systems, Helios also requires the least amount of unfamiliar, novel procedures. Essentially, the voter only has to interact with a series of webpages to vote. In contrast, with PaV voters have to tear their completed ballot in half, shred a portion of it, and then scan what is leftover into a scanner. Scantegrity II is similarly unique, requiring voters to use decoder pens, record revealed invisible ink codes, and then scan in their ballot. Deviations from the norm can hurt performance and user assessment of that system, which is reflected in our results. Furthermore, PaV and Scantegrity both require that candidate order be randomized, which violates the expectations of most voters and does not conform to election laws in most U.S. jurisdictions.

Even though voters have never seen or interacted with systems like these before, it should not be argued that high rates of failure to cast a vote or to verify a vote are to be expected—hence being acceptable in a system deployed for use. This argument can be countered in two ways. First, completion rates for two previously tested experimental voting systems—IVR and mobile vote—do not suffer from this phenomenon (Holmes & Kortum, 2013; Campbell et al., in press). Second, and more importantly, voting should be considered a walk-up-and-use activity. If a voter only votes in national elections, then there are four years between each interaction a voter has with a particular system, and learning retention is poor under infrequent exposures. Voters must be able to use the system with near 100% success with little or no experience or training.

3) Verification Output Is Not Automated, So Users Make Mistakes
Verification of a vote is a new feature of these systems, so this probably led to some of the system problems like not being able to verify or recognize that their vote had been verified. However, the benefits derived from this feature are so central to these enhanced security systems that more needs to be done to assist voters in the successful completion of this step. As noted, one of the great difficulties users faced is that they either failed to understand that they needed to record additional information to verify, or the additional labor involved dissuaded them from making the effort. Further, even if voters understood and wanted to perform these steps, the likelihood of committing errors in this step was high. Providing assistance to the voter, such as automated output of the ballot ID (which PaV did) or security codes might have made this step more tenable from the voter's standpoint.

4) Insufficient User Instructions
Because these e2e system are both relatively new and place additional cognitive burdens on the users, enhanced instruction may be required. This does not necessarily mean giving the voters long, detailed instructions for use at each station, as these were often ignored or skimmed in the systems tested here. It does mean providing specific, clear helping instructions at critical junctures in the process. Instructions should never be a substitute for good design, but occasionally, good inline dialogue can mitigate design features that are crucial to the systems operation. This lack of inline instruction may have been why subjective usability was lowest for Helios. Helios provided instructions in the beginning on how to vote, but after casting a ballot, the system did not tell the voter how they could follow up by verifying to be assured that their vote was handled correctly.

5) Voting Systems Were Not Specified in Detail
One of the things learned quickly as our team tried to construct these systems is that while the security mechanisms were well-specified by the researchers who imagined them, not every system specification was defined. This is understandable, as the papers we used to model e2e systems described the security and general functioning of the system, not every single operational user interface detail. However, anyone (like a county clerk) who wanted to implement such a system would be left to devise their own best practices for all the omitted details, and this could lead to a wide range of outcomes depending on the implementation. The devil is always in the details, and this is especially true for complex systems such as these. It also points to the need for enhanced collaboration between security researchers and human factors specialists when developing such systems.

Where do we go from here?
Despite the usability problems associated with the tested systems, one must keep in mind that they have the potential to be both more secure and more accurate than traditional voting systems once the systems are usable by everyone. Incorporating human factors research and development methods during active system development would be a critical part of ensuring that these types of systems are developed with the user in mind

There are numerous questions that future research should address. For example, are people with disabilities able to use the voter verifiable systems? If not, what can be done so that they can easily and quickly vote? Are the auditing portions of the system usable? When a voter verifies their vote with a system like Scantegrity II or PaV that displays their unique codes or images of their ballot, how accurate are voters? In other words, would people actually catch errors? How do voters report concerns about their verified votes? All three systems are designed to allow voters to check that things are working properly. But if they are not, what do voters do? By answering questions like these, the systems will be able to be further improved and the relationship between security and usability will be understood in more detail.

CONCLUSION
The data from this study serves as a reference point for future research and discussions about the usability of voter verifiable voting systems. It also enables e2e systems to be compared to other voting systems that have been previously tested or will be tested in the future. With that being said, this study only begins to answer basic research questions surrounding these new systems, while highlighting many avenues for future studies.

ACKNOWLEDGEMENTS
This research was supported in part by the National Institute of Standards and Technology under grant #60NANB12D249. The views and conclusions expressed are those of the authors and should not be interpreted as representing the official policies or endorsements, either expressed or implied, of NIST, the U.S. government, or any other organization.

REFERENCES

Adida, B. (2008). Helios: Web-based open-audit voting. *Proceedings of the 17th USENIX Security Symposium*, *USA, 17*, 335-348.

Adida, B., De Marneffe, O., Pereira, O., & Quisquater, J. J. (2009). Electing a university president using open-audit voting: Analysis of real-world use of Helios. *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections, USA, 18*.

Bangor, A., Kortum, P.T., Miller, J.T. (2008). An Empirical Evaluation of the System Usability Scale. *International Journal of Human-Computer Interaction, 24*(6), 574-594.

Benaloh, J. (2006). Simple verifiable elections. *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop, USA, 15.*

Brent, P. (2006). The Australian ballot: Not the secret ballot. *Australian Journal of Political Science, 41*(1), 39-50.

Brooke, J. (1996). SUS: A 'quick and dirty' usability scale. In P.W. Jordan, B. Thomas, B.A. Weerdmeester, & I.L. McCelland (Eds.), *Usability Evaluation in Industry* (pp. 189-194). Bristol: Taylor & Francis.

Byrne, M. D., Greene, K. G., & Everett, S. P. (2007). Usability of voting systems: Baseline data for paper, punchcards, and lever machines. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM* (pp. 171-180).

Burton, C., Culnane, C., Heather, J., Peacock, T., Ryan, P. Y., Schneider, S., ... & Xia, Z. (2012, July). Using Prêt a Voter in Victorian State elections. *Proceedings of the 2012 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections, USA, 21*.

Campbell, B. A., & Byrne, M. D. (2009). Now do voters notice review screen anomalies? A look at voting system usability. *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections, USA, 18*.

Campbell, B. A., Tossell, C. C., Byrne, M. D., & Kortum, P. (2011, September). Voting on a Smartphone Evaluating the Usability of an Optimized Voting System for Handheld Mobile Devices. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting: Vol. 55*(1). *Human Factors and Ergonomics Society* (pp. 1100-1104).

Campbell, B. A., Tossell, C. C., Byrne, M. D., Kortum, P. (in press). Toward more usable electronic voting: Testing the usability of a smartphone voting system. In *Human Factors.*

Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., ... Vora, P.L. (2010). Scantegrity II Municipal Election at Takoma Park: The first e2e binding governmental election with ballot privacy. *Proceedings of the 19th USENIX Security Symposium*, *USA, 19*.

Chain voting prevented by new ballots. (1931, August 27). *The Gettysburg Times,* p. 1.

Chaum, D. (2004). Secret ballot receipts: True voter-verifiable elections. *IEEE Security & Privacy, 2*(1), 38-47.

Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R. L., ... & Sherman, A. T. (2008). Scantegrity II: end-to-end verifiability for optical scan election systems using invisible ink confirmation codes. *Proceedings of EVT* '08, *USA*.

Chaum, D., Jakobsson, M., Rivest, R. L., Ryan, P. Y., Benaloh, J., & Kutylowski, M. (Eds.). (2010). *Lecture Notes in Computer Science: Vol. 6000. Towards Trustworthy Elections: New Directions in Electronic Voting.* New York, NY: Springer.

Clarkson, M. R., Chong, S. N., & Myers, A. C. (2008). Civitas: Toward a secure voting system. In *Proceedings of the 2008 IEEE Symposium on Security & Privacy. IEEE Computer Society* (pp. 354-368).

Everett, S. P. (2007). *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection* (Doctoral dissertation, Rice University). Retrieved from http://chil.rice.edu/alumni/petersos/EverettDissertation.pdf

Everett, S., Greene, K., Byrne, M., Wallach, D., Derr, K., Sandler, D., & Torous, T. (2008). Electronic voting machines versus traditional methods: Improved preference, similar

performance. In *Proceedings of the SIGCHI Conference onHuman Factors in Computing Systems. ACM* (pp. 883-892).

Holmes, D., & Kortum, P. (2013). Vote-By-Phone: Usability Evaluation of an IVR Voting System. In Proceedings of the *Human Factors and Ergonomics Society Annual Meeting: Vol. 57*(1). *Human Factors and Ergonomics Society* (pp. 1308-1312).

IACR. (n.d.). *Should the IACR Use E-Voting for Its Elections*? Retrieved from http://www.iacr.org/elections/eVoting/

ISO. (1998). *Ergonomic requirements for office work with visual display terminal (VDT's)–Part 11: Guidance on usability* (ISO 9241-11(E)). Geneva, Switzerland.

Jones, D.W. (2001). A brief illustrated history of voting. *Voting and Elections Web Pages.* Retrieved from http://homepage.cs.uiowa.edu/~jones/voting/pictures

Karayumak, F., Kauer, M., Olembo, M., Volk, T., & Vokamer, M. (2011). User study of the improved helios voting system interfaces. In *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. *IEEE Computer Society* (pp. 37-44).

Laskowski, S.J., Autry, M., Cugini, J., Killam, W., & Yen, J. (2004). Improving the usability and accessibility of voting systems and products. Washington: D.C.: National Institute of Standards and Technology. Retrieved from http://ucdwww.user.openhosting.com/ files/NISTHFReport.pdf

Lundin, D., & Ryan, P.Y. (2008). Human readable paper verification of Prêt à Voter. In S. Jajodia & J. Lopez (Eds.), *Computer Security – ESORICS 2008: Proceedings of the 13th European Symposium on Research in Computer Security, Malaga, Spain, October 6-8, 2008* (pp. 379-395). Berlin, Germany: Springer Berlin Heidelberg.

Masnick, M. (2008). Guy Who Insists E-Voting Machines Work Fine… Demonstrates They Don't. *Tech Dirt.* Retrieved from http://www.techdirt.com/articles/20081029/0131342676.shtml

Norden, L., Kimball, D., Quesenbery, W. & Chen, M. (2008). *Better Ballots*. New York: Brennan Center for Justice. Retrieved from https://www.supportthevoter.gov/files/2013/08/Better-Ballots-Brennan-Center.pdf

Prêt à Voter. (n.d.). Retrieved from http://www.pretavoter.com

Ryan, P. Y., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). Prêt à voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security, 4*(4), 662-673.

Ryan, P.Y., & Peacock, T. (2010). A threat analysis of Prêt à Voter. In D. Chaum, M. Jakobsson, R.L. Rivest, P.Y. Ryan, J. Benaloh, & M. Kutylowski, (Eds.), *Lecture Notes in Computer Science: Vol. 6000. Towards Trustworthy Elections: New Directions in Electronic Voting* (pp. 200-215). New York, NY: Springer.

Ryan, P.Y., & Schneider, S.A. (2006). Prêt à Voter with re-encryption mixes. In D. Gollmann, J. Meier, & A. Sabelfeld (Eds.), *Computer Security – ESORICS 2006: Proceedings of the 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20, 2006* (pp. 313-326). Berlin, Germany: Springer Berlin Heidelberg.

Sandler, D., Derr, K., & Wallach, D. S. (2008). VoteBox: A Tamper-evident, Verifiable Electronic Voting System. *Proceedings of the 17th USENIX Security Symposium*, *USA, 4*.

Sauro, J. (2011, February 2). Measuring usability with the system usability scale (SUS) [Web log post]. Retrieved from https://www.measuringusability.com/sus.php

Shackel, B. (1991). Usability-context, framework, definition, design and evaluation. In *Human Factors for Informatics Usability* (pp. 21-37). New York, NY: Cambridge University Press.

Weber, J., & Hengartner, U. (2009). *Usability study of the open audit voting system Helios*. Retrieved from http://www.jannaweber.com/wpcontent/uploads/2009/09/ 858Helios.pdf

Winckler, M., Bernhaupt, R., Palanque, P., Lundin, D., Ryan, P., Alberdi E., & Strigini, L. (2009). *Assessing the usability of open verifiable e-voting systems: a trial with the system Pret a Voter*. Retrieved from http://www.irit.fr/~Marco.Winckler/publications/2009-ICEGOV.pdf

Appendix 1--Helios Voting System Study Materials

General Election
Harris County, Texas
November 8, 2016

To participate in this election, you will need to use the internet. For voting instructions, please go to: **mail.google.com**

Login to Gmail using the following information:

Username: xraychicken

Password: suitandtie

Figure A1.1. Study instructions for the Helios mock-election

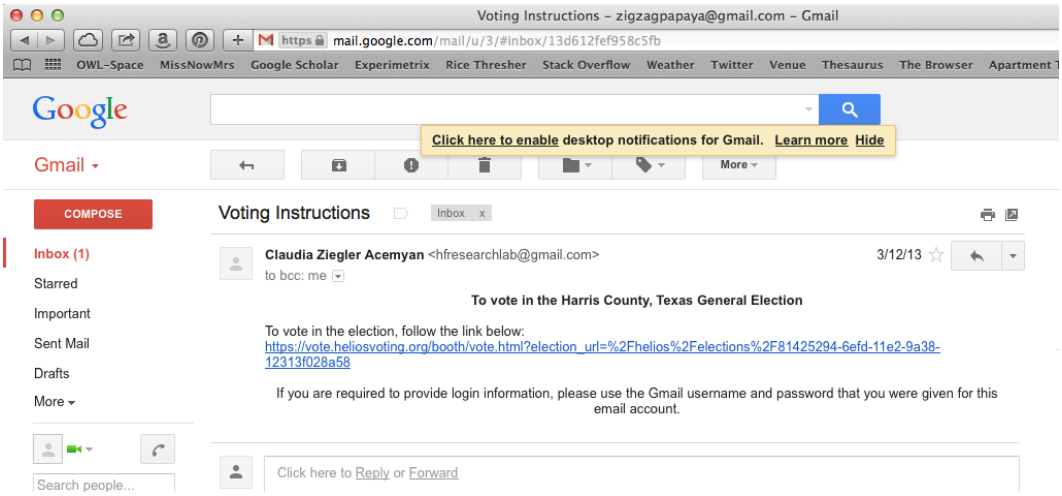


Figure A1.2. Screenshot of the emailed instructions and link to the Helios election

Appendix 1--Helios Voting System Study Materials

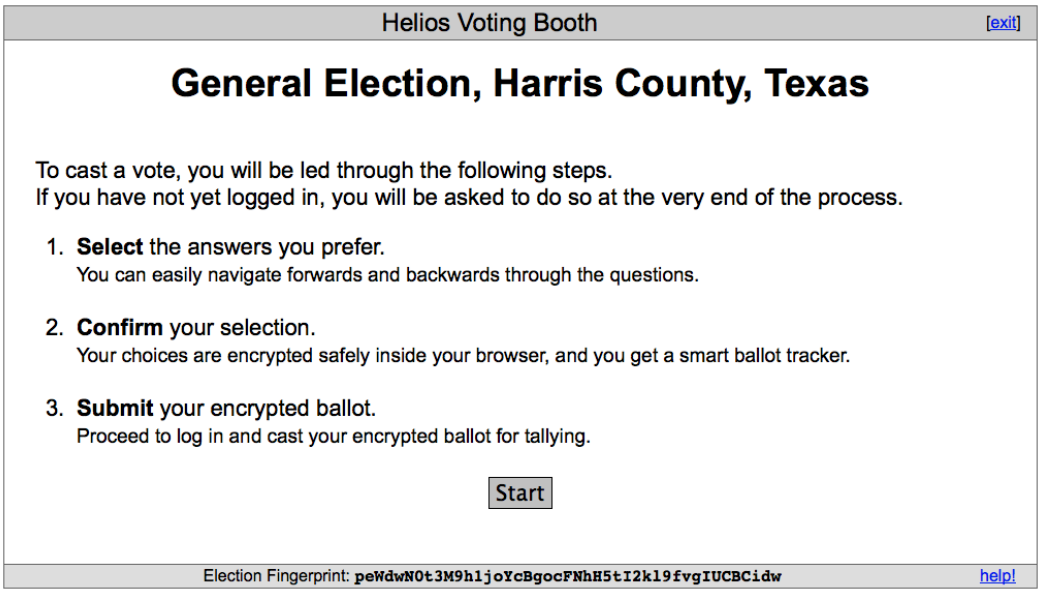


Figure A1.3. Screenshot of the Helios Voting Booth instructions

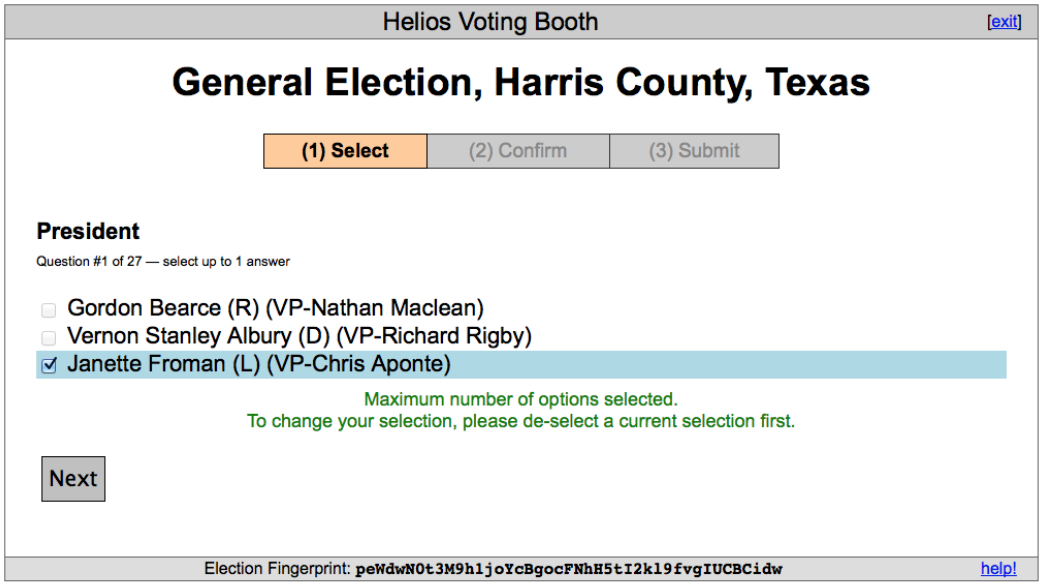
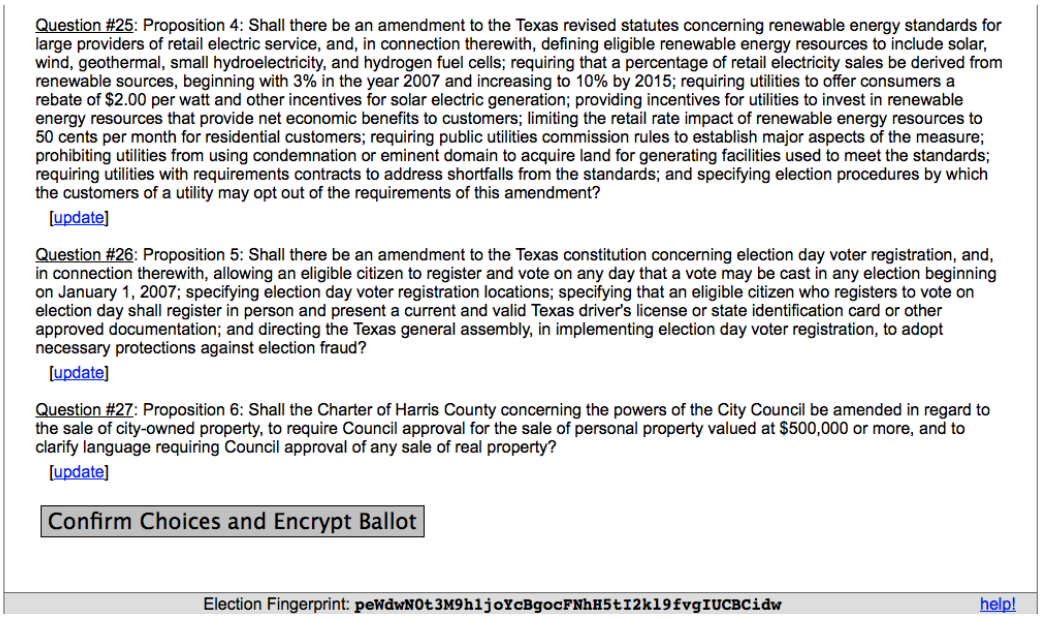


Figure A1.4. Screenshot of the presidential race on the Helios Ballot

Appendix 1--Helios Voting System Study Materials



Question #25: Proposition 4: Shall there be an amendment to the Texas revised statutes concerning renewable energy standards for large providers of retail electric service, and, in connection therewith, defining eligible renewable energy resources to include solar, wind, geothermal, small hydroelectricity, and hydrogen fuel cells; requiring that a percentage of retail electricity sales be derived from renewable sources, beginning with 3% in the year 2007 and increasing to 10% by 2015; requiring utilities to offer consumers a rebate of $2.00 per watt and other incentives for solar electric generation; providing incentives for utilities to invest in renewable energy resources that provide net economic benefits to customers; limiting the retail rate impact of renewable energy resources to 50 cents per month for residential customers; requiring public utilities commission rules to establish major aspects of the measure; prohibiting utilities from using condemnation or eminent domain to acquire land for generating facilities used to meet the standards; requiring utilities with requirements contracts to address shortfalls from the standards; and specifying election procedures by which the customers of a utility may opt out of the requirements of this amendment?

[update]

Question #26: Proposition 5: Shall there be an amendment to the Texas constitution concerning election day voter registration, and, in connection therewith, allowing an eligible citizen to register and vote on any day that a vote may be cast in any election beginning on January 1, 2007; specifying election day voter registration locations; specifying that an eligible citizen who registers to vote on election day shall register in person and present a current and valid Texas driver's license or state identification card or other approved documentation; and directing the Texas general assembly, in implementing election day voter registration, to adopt necessary protections against election fraud?

[update]

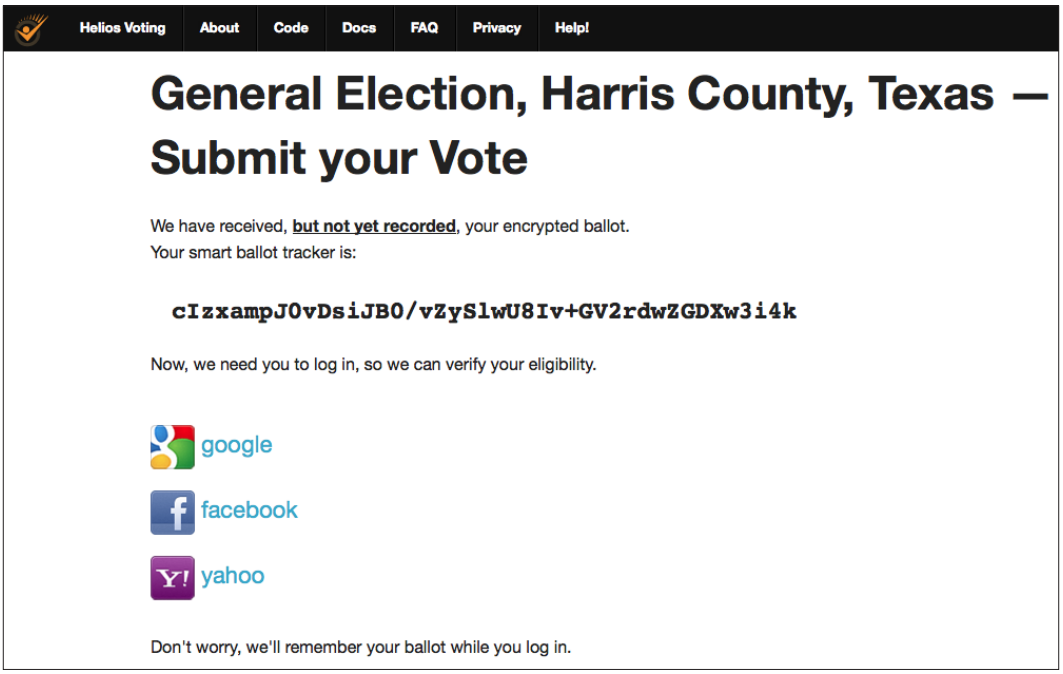
Question #27: Proposition 6: Shall the Charter of Harris County concerning the powers of the City Council be amended in regard to the sale of city-owned property, to require Council approval for the sale of personal property valued at $500,000 or more, and to clarify language requiring Council approval of any sale of real property?

[update]

Confirm Choices and Encrypt Ballot

Election Fingerprint: **peWdwN0t3M9h1joYcBgocFNhH5tI2kl9fvgIUCBCidw** help!

Figure A1.5. Screenshot of the Helios review screen



Helios Voting | About | Code | Docs | FAQ | Privacy | Help!

General Election, Harris County, Texas — Submit your Vote

We have received, **but not yet recorded**, your encrypted ballot.
Your smart ballot tracker is:

cIzxampJ0vDsiJB0/vZySlwU8Iv+GV2rdwZGDXw3i4k

Now, we need you to log in, so we can verify your eligibility.

google

facebook

yahoo

Don't worry, we'll remember your ballot while you log in.

Figure A1.6. Screenshot of one Helios vote submission page

Appendix 1--Helios Voting System Study Materials

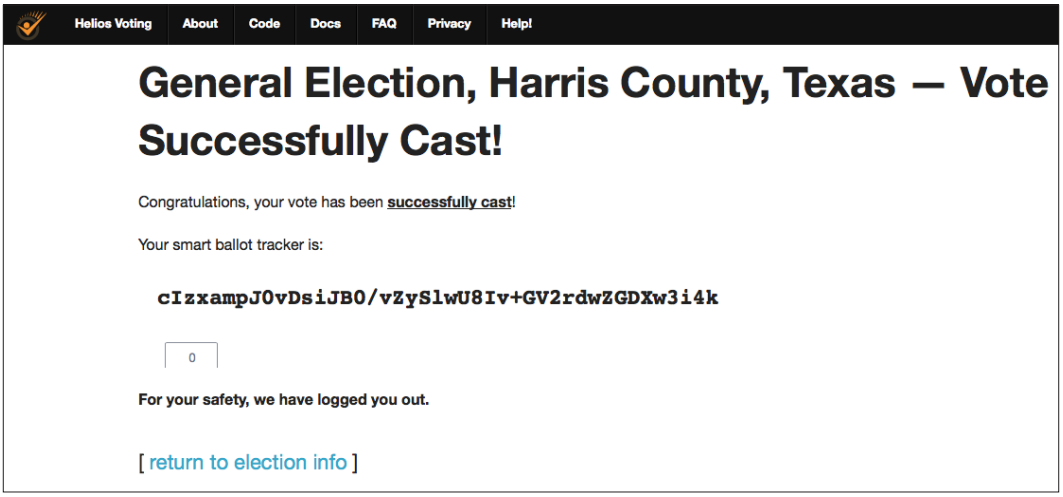


Figure A1.7. Screenshot of the Helios cast vote confirmation page, which is shown at the end of the voting process

red monkey	x/hVL7Yg/F4cQ6t12d4WfdmaV4wDUKNcTkqEWPP7CPA	[view]
Participant 83	5vWdkhyE849pE9sC5lzY+CBURhMlhccW7WGYN6IBR2A	[view]
Participant 74	X1OeO8i1giZ7q50jjdwNO2FNi7ltXEfhjb8lABwRhSA	[view]
Participant 80	V9eoWPeDJL75wPOyr6qH4dyKZzhdNNYo8qcbUj7pMsI	[view]
Human Factors	0WdUOUZrVb+QbVhMzuLLI+ENQcXdv3pbjWIjoXcadh4	[view]
Participant 10	DjxiWadCamDcgG8qMA+bNWTZ3aDiEDgW71Bx0laLaw8	[view]
Participant 11	7Xt6BNmnGZwy2FatxHgWAeVdEEQo9kQ5usIkwPmfYC8	[view]
Participant 14	—	
Participant 17	gpyTOMwLAJ1+QIWeHSZlT05GtRu0w509gPvHk/831W4	[view]
Participant 18	IpGY4e+mT7Qfz0WNiwzj5RPWgt2JcS/y+8YG9BOJtXo	[view]
Participant 1	LnTLOEz0D5TlWVcWTAY1wCjNnzBPAlxxrTplygHxaqI	[view]
Participant 4	WLselSilhPcvGq96EFFLVgI8Br6whgT+qaykLH+LXSM	[view]
Human Factors	b0pUYLZ7EdLORbJilksjjwz9/Vnr1Jxs96kUaj03NqA	[view]
yellow owl	/WMZXEAOH1Itj7bLJZoLOfl2R5jrI36aKliWwhqmVLI	[view]
Participant 23	cIzxampJ0vDsiJB0/vZySlwU8Iv+GV2rdwZGDXw3i4k	[view]

Figure A1.8. Screenshot of Helios' Voters and Ballot Tracking Center

Appendix 1--Helios Voting System Study Materials

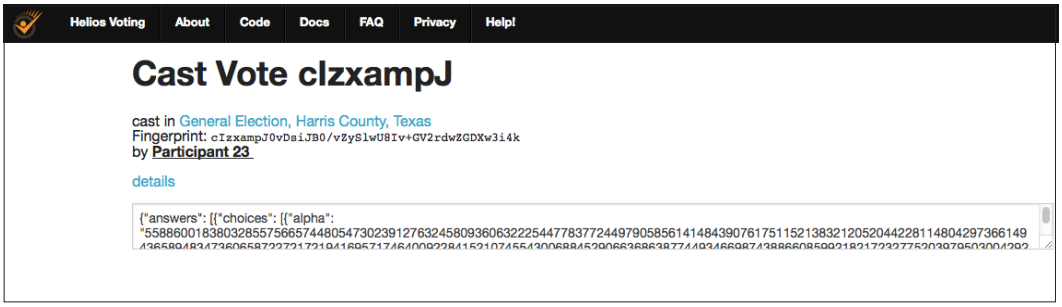


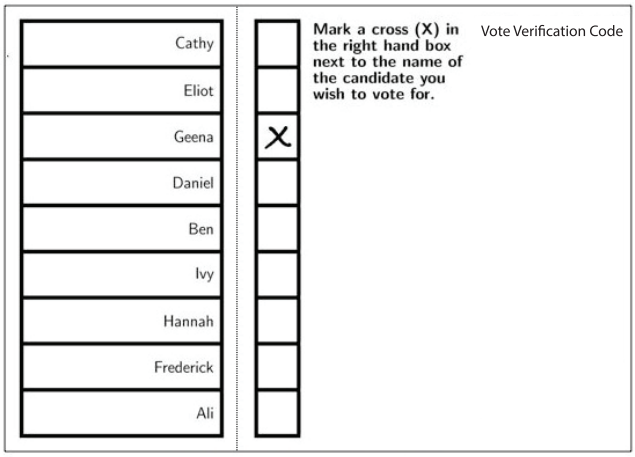
Figure A1.9. Screenshot of a voter's archived ballot (accessed by voter through the emailed cast ballot confirmation link)

Appendix 2--Pret a Voter Voting System Study Materials

General Election Ballot
Harris County, Texas
November 8, 2016

INSTRUCTIONS TO VOTERS

1. Mark a cross (x) in the right hand box next to the name of the candidate you wish to vote for. For an example, see the completed sample ballot below. Use only the marking device provided or a number 2 pencil. Please note that this ballot has multiple cards. If you make a mistake, don't hesitate to ask for a new ballot. If you erase or make other marks, your vote may not count.



2. After marking all of your selections, detach the candidates lists (left side of cards).

3. Shred the candidates lists.

4. Feed your voting slips into the scanner.

5. Take your receipts. Receipts can be used to confirm that you voted by visiting votingstudy.rice.edu.

Figure A2.1. Voting Instructions for PaV

Appendix 2--Pret a Voter Voting System Study Materials

PRESIDENT AND VICE PRESIDENT

Card Key: **7rJ94K-1**

Card 1 of 8

President and Vice President
Vote for One

REP	Gordon Bearce Nathan Maclean	
DEM	Vernon Stanley Albury Richard Rigby	
LIB	Janette Froman Chris Aponte	

Mark a cross (X) in the right hand box next to the name of the candidate you wish to vote for.

CONGRESSIONAL

United States Senator
Vote for One

REP	Cecile Cadieux	
DEM	Fern Brzezinski	
IND	Corey Dery	

Representative in Congress, District 7
Vote for One

REP	Pedro Brouse	
DEM	Robert Mettler	

STATE

Governor
Vote for One

REP	Glen Travis Lozier	
DEM	Rick Stickles	
IND	Maurice Humble	

Card 1 of 8

Ballot Continues on Card 2

Figure A2.2. Card 1/8 of the PaV ballot

Appendix 2--Pret a Voter Voting System Study Materials

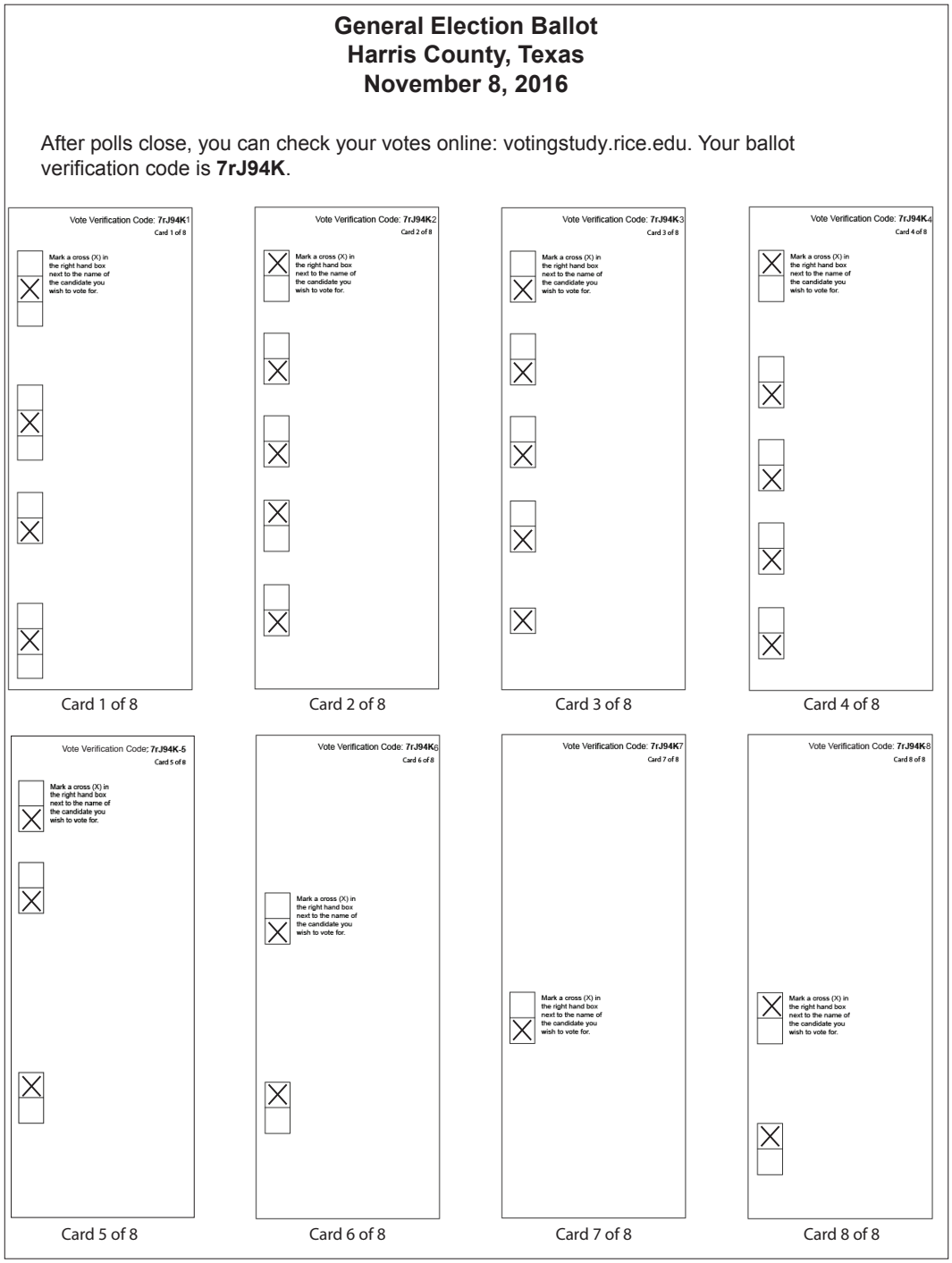
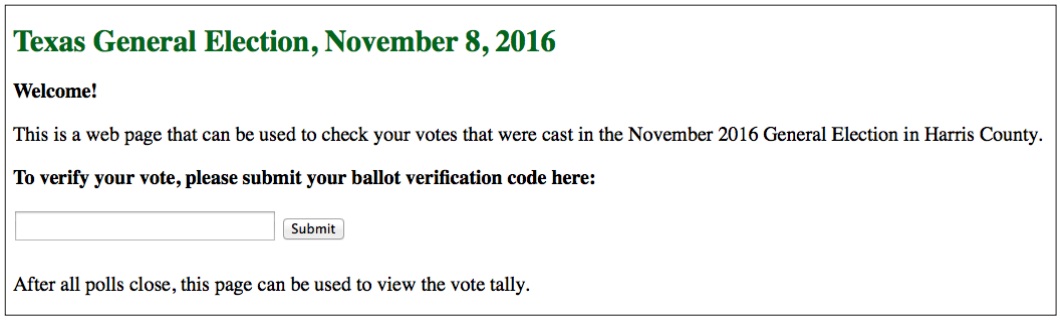


Figure A2.3. PaV voter receipt

Appendix 2--Pret a Voter Voting System Study Materials



Texas General Election, November 8, 2016

Welcome!

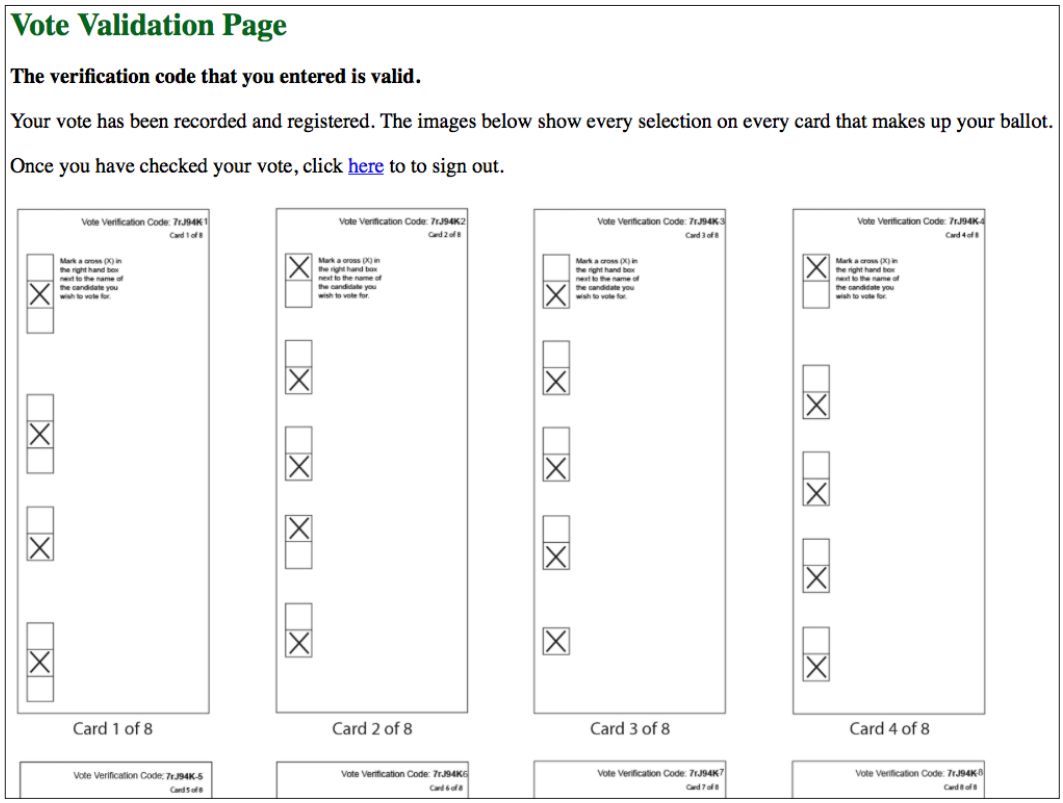
This is a web page that can be used to check your votes that were cast in the November 2016 General Election in Harris County.

To verify your vote, please submit your ballot verification code here:

Submit

After all polls close, this page can be used to view the vote tally.

Figure A2.4. Screenshot of PaV's vote verification web page (site homepage)



Vote Validation Page

The verification code that you entered is valid.

Your vote has been recorded and registered. The images below show every selection on every card that makes up your ballot.

Once you have checked your vote, click here to to sign out.

Card 1 of 8 | Card 2 of 8 | Card 3 of 8 | Card 4 of 8

Figure A2.4. Screenshot of PaV's vote validation web page

Appendix 3--Scantegrity II Voting System Study Materials

GENERAL ELECTION BALLOT
HARRIS COUNTY, TEXAS
NOVEMBER 8, 2016

- TO VOTE, COMPLETELY FILL IN THE OVAL ⬬ NEXT TO YOUR CHOICE.
- Use only the special marking device provided.
- If you make a mistake, do not hesitate to ask for a new ballot. If you make other marks, your vote may not count.
- A confirmation number will appear inside the oval you mark. You may later use this confirmation number to verify your vote online. After marking the ballot, you may choose to write down your confirmation numbers on the card provided in the voting booth.
- To cast your vote, take your ballot to the scanner. Keep the card to verify your vote online after the polls close.

PRESIDENT AND VICE PRESIDENT

PRESIDENT AND VICE PRESIDENT
(Vote for One)

- ◯ Gordon Bearce / Nathan Maclean — REP
- ◯ Vernon Stanley Albury / Richard Rigby — DEM
- ◯ Janette Froman / Chris Aponte — LIB

CONGRESSIONAL

UNITED STATES SENATOR
(Vote for One)

- ◯ Cecile Cadieux — REP
- ◯ Fern Brzezinski — DEM
- ◯ Corey Dery — IND

REPRESENTATIVE IN CONGRESS
(Vote for One)

- ◯ Pedro Brouse — REP
- ◯ Robert Mettler — DEM

STATE

GOVERNOR
(Vote for One)

- ◯ Glen Travis Lozier — REP
- ◯ Rick Stickles — DEM
- ◯ Maurice Humble — IND

LIEUTENANT GOVERNOR
(Vote for One)

- ◯ Shane Terrio — REP
- ◯ Cassie Principe — DEM

ATTORNEY GENERAL
(Vote for One)

- ◯ Tim Speight — REP
- ◯ Rick Organ — DEM

COMPTROLLER OF PUBLIC ACCOUNTS
(Vote for One)

- ◯ Therese Gustin — IND
- ◯ Greg Converse — DEM

STATE

COMMISSIONER OF GENERAL LAND OFFICE
(Vote for One)

- ◯ Sam Saddler — REP
- ◯ Elise Ellzey — DEM

COMMISSIONER OF AGRICULTURE
(Vote for One)

- ◯ Polly Rylander — REP
- ◯ Roberto Aron — DEM

RAILROAD COMMISSIONER
(Vote for One)

- ◯ Jillian Balas — REP
- ◯ Zachary Minick — DEM

STATE SENATOR
(Vote for One)

- ◯ Ricardo Nigro — REP
- ◯ Wesley Steven Millette — DEM

STATE REPRESENTATIVE DISTRICT 134
(Vote for One)

- ◯ Petra Bencomo — REP
- ◯ Susanne Rael — DEM

MEMBER
STATE BOARD OF EDUCATION
DISTRICT 2
(Vote for One)

- ◯ Peter Varga — REP
- ◯ Mark Barber — DEM

PRESIDING JUDGE
TEXAS SUPREME COURT
PLACE 3
(Vote for One)

- ◯ Tim Grasty — DEM

PRESIDING JUDGE
COURT OF CRIMINAL APPEALS, PLACE 2
(Vote for One)

- ◯ Dan Plouffe — REP
- ◯ Derrick Melgar — DEM

COUNTY

DISTRICT ATTORNEY
(Vote for One)

- ◯ Corey Behnke — REP
- ◯ Jennifer A. Lundeed — DEM

COUNTY TREASURER
(Vote for One)

- ◯ Dean Caffee — REP
- ◯ Gordon Kallas — DEM

SHERIFF
(Vote for One)

- ◯ Stanley Saari — GP
- ◯ Jason Valle — LIB

COUNTY TAX ASSESSOR
(Vote for One)

- ◯ Howard Grady — IND
- ◯ Randy H. Clemons — CON

NONPARTISAN

JUSTICE OF THE PEACE
(Vote for One)

- ◯ Deborah Kamps
- ◯ Clyde Gayton Jr.

COUNTY JUDGE
(Vote for One)

- ◯ Dan Atchley
- ◯ Lewis Shine

PROPOSITIONS

PROPOSITION 1

Without raising taxes and in order to pay for public safety, public works, parks and recreation, health care, libraries, and other essential services, shall Harris County and the City of Houston be authorized to retain and spend all city and county tax revenues in excess of the constitutional limitation on total city and county fiscal year spending for ten fiscal years beginning with the 2011 fiscal year, and to retain and spend an amount of city and tax revenues in excess of such limitation for the 2020 fiscal year and for each succeeding fiscal year up to the excess city and county revenue cap, as defined by this measure?

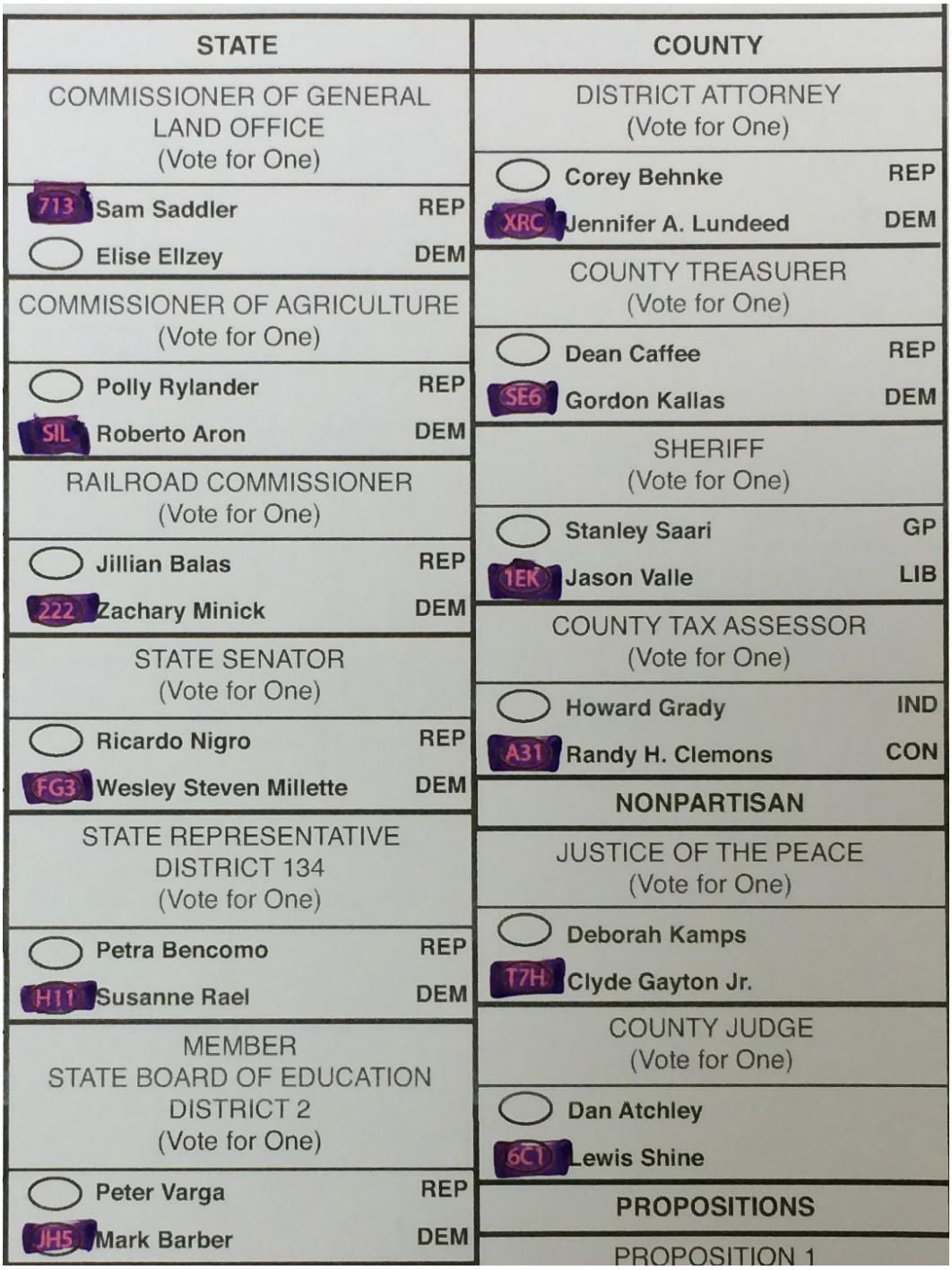
- ◯ YES
- ◯ NO

VOTE BOTH SIDES OF BALLOT

Ballot ID / Online Verification Number
HC-2016-11-08-420795502

Figure A3.1. Scantegrity II ballot

Appendix 3--Scantegrity II Voting System Study Materials



STATE

COMMISSIONER OF GENERAL LAND OFFICE
(Vote for One)

713 Sam Saddler REP
Elise Ellzey DEM

COMMISSIONER OF AGRICULTURE
(Vote for One)

Polly Rylander REP
SIL Roberto Aron DEM

RAILROAD COMMISSIONER
(Vote for One)

Jillian Balas REP
222 Zachary Minick DEM

STATE SENATOR
(Vote for One)

Ricardo Nigro REP
FG3 Wesley Steven Millette DEM

STATE REPRESENTATIVE DISTRICT 134
(Vote for One)

Petra Bencomo REP
H11 Susanne Rael DEM

MEMBER STATE BOARD OF EDUCATION DISTRICT 2
(Vote for One)

Peter Varga REP
JH5 Mark Barber DEM

COUNTY

DISTRICT ATTORNEY
(Vote for One)

Corey Behnke REP
XRC Jennifer A. Lundeed DEM

COUNTY TREASURER
(Vote for One)

Dean Caffee REP
SE6 Gordon Kallas DEM

SHERIFF
(Vote for One)

Stanley Saari GP
1EK Jason Valle LIB

COUNTY TAX ASSESSOR
(Vote for One)

Howard Grady IND
A31 Randy H. Clemons CON

NONPARTISAN

JUSTICE OF THE PEACE
(Vote for One)

Deborah Kamps
T7H Clyde Gayton Jr.

COUNTY JUDGE
(Vote for One)

Dan Atchley
6C1 Lewis Shine

PROPOSITIONS

PROPOSITION 1

Figure A3.2. Photograph of a completed Scantegrity II ballot, with invisible ink confirmation codes revealed

Appendix 3--Scantegrity II Voting System Study Materials

INSTRUCTIONS FOR VERIFYING YOUR VOTE ON-LINE AFTER YOU RETURN HOME

You have the **OPTION** of verifying your vote on-line after you return home. **It is not necessary to do so.** You may ignore this step entirely; **your cast ballot will be counted whether or not you do this verification process.**

If you wish to verify your vote on-line, perform the following steps:

1. Fill out your ballot according to the instructions provided on the ballot. "Confirmation numbers" will appear inside the oval you mark.

2. **BEFORE** YOU CAST YOUR BALLOT record the Online Verification Number and the confirmation numbers below, using the special pen.

"On-Line Verification Number" from the bottom right corner of your ballot:

Race	Code
President And Vice President	
United States Senator	
Representative in Congress	
Governor	
Lieutenant Governor	
Attorney General	
Comptroller of Public Accounts	
Commissioner of General Land Office	
Commissioner of Agriculture	
Railroad Commissioner	
State Senator	
State Representative District 134	
Member State Board of Education, District 2	

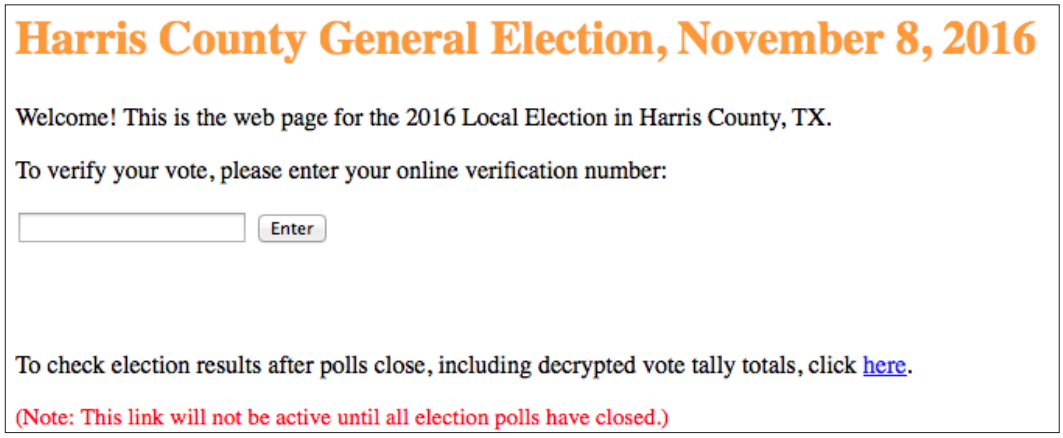
Race	Code
Judge Texas Supreme Court	
Judge Court of Criminal Appeals	
District Attorney	
County Treasurer	
Sheriff	
County Tax Assessor	
Justice of the Peace	
County Judge	
Proposition 1	
Proposition 2	
Proposition 3	
Proposition 4	
Proposition 5	
Proposition 6	

3. **Cast your ballot as usual using the polling station's scanner. DO NOT CAST THIS SHEET, but take it home with you.**

4. After you have returned home, use a computer with an Internet connection to access the County's vote verification web page: **mockelection.rice.edu**. Here you will see instructions for verifying that the confirmation numbers you wrote down are correctly recorded. Note that the confirmation numbers are randomly generated and cannot be used to determine how you voted.

Figure A3.3. Scantegrity II vote verification sheet

Appendix 3--Scantegrity II Voting System Study Materials



Harris County General Election, November 8, 2016

Welcome! This is the web page for the 2016 Local Election in Harris County, TX.

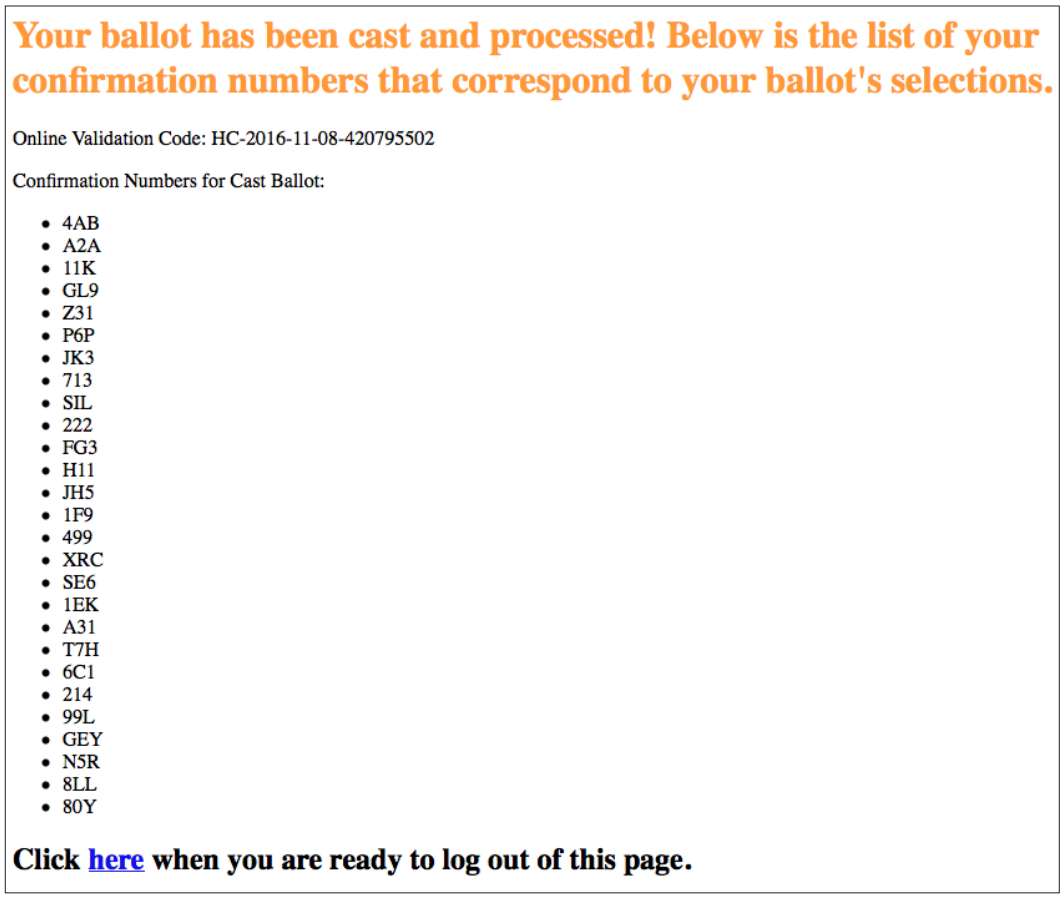
To verify your vote, please enter your online verification number:

Enter

To check election results after polls close, including decrypted vote tally totals, click here.

(Note: This link will not be active until all election polls have closed.)

Figure A3.4. Screenshot of Scantegrity II vote verification page (site homepage)



Your ballot has been cast and processed! Below is the list of your confirmation numbers that correspond to your ballot's selections.

Online Validation Code: HC-2016-11-08-420795502

Confirmation Numbers for Cast Ballot:

- 4AB
- A2A
- 11K
- GL9
- Z31
- P6P
- JK3
- 713
- SIL
- 222
- FG3
- H11
- JH5
- 1F9
- 499
- XRC
- SE6
- 1EK
- A31
- T7H
- 6C1
- 214
- 99L
- GEY
- N5R
- 8LL
- 80Y

Click here when you are ready to log out of this page.

Figure A3.5. Screenshot of Scantegrity II cast ballot confirmation page