Voting, Vote Capture & Vote Counting Symposium

Annotated Best Practices

The following is a set of annotated best practices developed at the Vote, Vote Capture and Vote Counting Symposium at the Kennedy School of Government. These best practices are offered and have been annotated for the use of citizens, technologists, and the election officials who endeavor to serve them. This set of best practices is written as a summary document. Although not every attendee will agree with every best practice, these recommendations fairly reflect the overall conclusions.

The best practices alone provide a terse but useful checklist for developing and maintaining a flexible but trustworthy voting system in the information age. The annotated best practices clarifies and comments on the best practices based on the notes of the Symposium and the discussion of the shorter document.

1. Certain Immediate Steps Must Be Taken.

In the long term the contested arenas of corporate governance and technology policy are intertwined with the administration of highly contested elections. However, with the 2004 Presidential Election fast approaching, it is important to prioritize. Certain actions can and must be started now, both for 2004 and beyond.

1.1 Election Assistance Commission and National Institute of Standards and Technology open standards must be developed and implemented.

The Help America Vote Act (HAVA)1 provides funds, which are heavily subsidized by federal grants awarded by the newly formed US Election Assistance Commission, for the purchase of machines. The function of reviewing voting technology and development of standards under HAVA was assigned to a Technical Guidelines Development Committee (TGDC). Between October 2002 and now, under the proposed leadership of the Director of the National Institute of

[1] Help America Vote Act of 2022 (HAVA), Public Law No. 107-252, 116 Stat. 1666, available at http://www.fec.gov/hava/law_ext.txt

Standards and Technology (NIST),2 the TGDC could have taken significant steps toward the development of rigorous testing and certification processes for electronic voting technology. Unfortunately, efforts to developed and implement standards have been hindered by lack of funds and a slow start to the process. The standardization process must be well funded, bringing aboard qualified experts, and should attempt to expedite the process as much as possible.

EAC and NIST voting standards must be open and freely implementable. Anyone should be able to gain access to these standards to ascertain how much security they guarantee, or whether a specific technology is in compliance. They must be freely implementable so that any qualified individual can design a system that meets EAC standards. This not only aids in ensuring a competitive market and thus responsive vendors; it can help with popular perceptions of trust.

1.2 Voting experts and technologists can aid in whatever voting process is used by designing guides, working in polls and gathering trustworthy data.

As advanced technology is increasingly used in elections, the need for computer literate participants in the process is critical. Information technology experts from across state and local government should be made available to voting officials. The trust that the current process requires election officials place in vendors is not appropriate.

Independent auditing organizations should be truly independent. The most independent audit is by the informed and committed citizen computer professional.

2. A hybrid of paper and electronic systems provides an effective voting system.

No technology can solve every problem and mitigate every risk. However, a hybrid of paper ballots and electronic marking systems can capture the benefits of each while avoiding the pitfalls inherent in relying on one or the other. The ideal system depends on best

[2] National Institute of Standards and Technology http://vote.nist.gov/faq.html

attributes of each, and use modular construction that allows for simple integration of the two parts.

2.1 Electronic interfaces enable customizable ballots by zip code, party or disability.

An advantage electronic vote-selection systems is the programmable interface that is fully adaptable to a wide range of needs. Such flexibility can accommodate local or individuals needs, as well as particular demands of a given election. From a cost perspective, it may be cheaper for a larger jurisdiction to customize the interface for voters than distribute separate ballots of appropriate precincts in appropriate languages with appropriate features (e.g., print size). An electronic interface can also offer interactivity, and enable the voter to cast the ballot he or she intends. A smart system can check for undervotes or overvotes and can inform the voter that the ballot may be recorded as such, in time for the voter to alter his or her selection before creating a finalized ballot.

That electronic interfaces are flexible does not mean that they are optimal. For example, the widely criticized butterfly ballot could easily be reproduced on a screen. Taking advantage of the flexibility in interface design requires a process that includes usability testing.

2.2 Electronic Interfaces can meet the widest range of accessibility needs.

Recent tests and interviews have shown that many enjoy using an electronic interface in the voting process. Voters' comments regarding their experience with DRE voting machines are reported as being "great," "very easy," and "fast".3 Moreover, the customizability means that language or special need does not have to be an impediment. The existing Federal accessibility guidelines and the World Wide Web

[3] McCaffrey, Raymond and Barr, Cameron W. "Debut of New Technology Gets Mostly High Marks" The Washington Post. Found at: http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A24780-2004Mar2&notFound=true March 3, 2004; Page B04

usability guidelines offer a minimum set that allows for access; but neither standard assures usability.

Language and special need ballots increase the need for complete usability testing. All possible configurations should be tested before placing the voting system in the field. Any time that is saved in printing is more than required for accessibility and usability testing.

2.3 Voter verification of a paper ballot allows the greatest degree of confidence that the ballot was cast as intended.

A paper ballot can be visually or possibly physically examined by the voter, which can create a greater degree of trust. A human-readable ballot allows the voter to be certain that the ballot cast was what the voter intended before casting it. The voter should be able to dispose of the ballot and start anew if the ballot does not meet his or her standards.

Under no circumstances should the voter be able to leave the polling place with a ballot containing evidence of the vote. Additional mechanisms to read and verify the ballots are optimal to ensure the privacy of voters with special needs; automatic auditory ballot readers for the visually impaired, for example. If machine-readable information such as bar-codes exist on the ballot, electronic readers should be made available so that the citizen can interpret and interpret them.

2.3 A paper ballot, when handled properly, allows a robust audit trail for a recount to ensure that the ballot was count as cast.

As discussed below, audibility is a crucial component of any election. Auditing requires an independent tallying mechanism, and digital technology does not offer the best solution in this case, since digital content can be tampered with or erased on a much larger scale. Electronic vote tallies can be adjusted at a single juncture, while each ballot must be altered or destroyed in order to foil an auditing effort. Independent non-aggregated artifacts such as standard paper ballots are needed. Moreover, paper ballots can be counted and recounted by hand which, while potentially less than efficient, removes the need to rely on electronic counting machines for auditing.

2.4 Hybrid systems can be designed to accommodate provisional arrangements and contingencies for equipment failure.

There are many possible implementations of a hybrid system. If voter-verifiable ballots are available at the polling place, then voters can still cast their ballots directly on the voting stock. Voters of unknown registration status can still cast their vote using the same system as others, and their eligibility can be confirmed before the ballot is entered into the final count.

The system could revolve around an Optical Character Recognition (OCR) engine with a ballot reader and a ballot marker. Alternatively, a general-purpose computer with a printer could satisfy many needs, as could a standard Digital Recording Electric device (DRW) with a printer attached. Several key studies have urged a multi-stage architecture with complete separation between casting, validating and submitting vote for count.

3. The Process Is As Important As The Underlying Technology.

The process of executing the election is at least as important as the underlying technology. Perfect technology cannot repair a fundamentally flawed process. Adequate policies, institutions and people are needed to make sure that the voting systems are properly used. In every digital technology, particularly security technologies, the human factor is a critical component. The process and people requires investment equal to that of the investment in the technology. There are certain inherent trade-offs in the process that the technology may obscure but does not resolve.

3.1 Poll workers should be well trained to fully understand the technology and how to handle contingencies.

The poll workers are the voters first and, in most cases, only assistance in navigating the voting process. When introducing new technology to the polling place, the poll workers must bee well equipped to assist the voters in any way, as well as be prepared to respond to any problems that may arise. Training the poll workers is a large undertaking, as is training the officials who will be teaching the poll workers. These time constraints must be reflected in the schedule of deployment for any new system. Poll workers must be aware of what they might face, and given the tools to address as many of them as possible. This may include handling the voting systems themselves, but also understanding how the systems are to be operated in special cases, such as power failure, provisional voting and voters with special needs.

One option discussed at the symposium is an adaptation of the jury pool system. Such a system could rely upon voter registration list, and could be modified for a new poll worker poll program. Those participating in any poll worker pool will receive monetary compensation for two days, which should include 1 day of training and Election Day. In addition, poll workers should receive three years of exemption from both jury service and poll duty. As an incentive those who volunteer could receive five years of exemption from jury service or poll duty.

Another alternative, one that has proven successful in New York, is to directly recognize the value of poll workers with increased and generous renumeration. Payments on the order of hundreds instead of tens of dollars allows election officials to choose from competitive applications to be poll workers.

3.2 The educational process for given technologies must follow a "chain of trust" where the election workers trust their trainers and are trusted by the public.

If the voting system is not understood or trusted by the poll workers, they will not be able to adequately serve the public. All those participating in the election management process must have a good understanding of how the voting system works, and how each component helps ensure a well-run election. One major concern is the generational gap between the poll workers who volunteer and the professionals who maintain the computer equipment that may be foreign to the volunteers. Poll worker training must be designed to address this concern, and try to minimize discomfort or worries.

An adaptation of the jury pool system currently used to satisfy the legal requirements of jury trials, that relies upon voter registration list could be modified for a new poll worker poll program. Those participating in any poll worker pool will receive monetary compensation for two days, which should include 1 day of training and Election Day. In addition, poll workers should receive three years of exemption from both jury service and poll duty. As an incentive those who volunteer could receive five years of exemption from jury service or poll duty.

3.3 Poll workers should be well chosen from a motivated pool with incentives and monetary incentives have proven to work.

It is not enough to train poll workers: they must be motivated, responsible and competent. Compensation for the job has always been modest, but experience has shown that increasing the reward for serving a poll worker can yield a more capable pool of applicants. Other possible incentives include greater publicity and public acknowledgement of the work done, or even exemption from jury duty.

A very effective public relations campaign could be generated to increase the desire of registered voters to work at polling places on Election Day. Athletes, musicians, actors, etc, can be enlisted as Election Day workers. The public awareness campaign theme could be: You never know who you might see working at the polls on Election Day. The added benefit may also be higher voter participation by younger voters. A pilot project would be effective in testing out ways to improve the response to the community need of poll workers to service in local elections

3.4 Poll workers should not have to rely solely on the vendors to address observed errors.

Problems should not be dealt with by the same party that had responsibility for preventing their occurrence. Reliance on the vendors can create conditions for lock-in, if the jurisdiction is dependent on the vendor. Open or standardized systems should allow the local officials or an independent contractor to intervene when necessary. No one should be able to tinker with a certified voting system without full supervision.

3.5 There should be adequate time for determining the official tally.

It is critical to make sure every vote counts. Provisional ballots may need to be evaluated and added in, and the process should be assessed after the fact for irregularities. If necessary, and audit should take place soon after the election, and should be completed quickly. The official tally must be released soon after the election.

3.6 Speed and accuracy in the process are both achievable, but not simultaneously possible.

Fast counts necessarily exclude provisional votes; cannot include time to not examine ballots for undervotes; and do not include time examination of contested results.

The public should be educated about the distinction between the speed that allows immediate returns, and the accuracy required in the official tally.

There is no way to get a guaranteed fast tally, and a count that is as accurate as possible is the final goal. The public must understand that every vote counts, and should be counted. Promises or expectations of quick resolutions should be avoided, and the media should not overly stress preliminary counts. If a preliminary, uncertified tally is spread publicly, then contradicting that news can decrease confidence in the election.

3.7 There should be provisional voting mechanisms, and adequate time to evaluate provisional votes for the final tally.

Full information should exist about voter eligibility, but it is not always easy to get that information to the polls, and for that information to be up-to-date. Moreover, sometimes voters dispute their disenfranchised designation, and should have the ability to vote if the matter can be resolved in the matter of days. Those who avail themselves of provisional ballots should have access to the other features of the voting system, including accessibility and verifiability tools.

3.8 There is an inevitable tradeoff between authentication of voters and access.

Requiring greater proof of the right to vote will prevent some from voting; removing any requirement for proof will allow those without the right to vote to cast ballot. Robust authentication has proven to be a complex problem because, among other reasons, databases contain errors and are corruptible through the human element. The fact that there are inevitably errors in databases means that human judgments are still required. A database sometimes simply provides the wrong answer more quickly. Attention needs to be paid to any widespread bias that results from the balance between authentication or access.

4. Good Voting Systems Require Good Design Standards

Technological systems can and do embed values; this is best acknowledged through design standards and review processes. Technology is rarely neutral. Biases can be direct (disenfranchising those with special needs) or persuasive (making one vote easier than another to cast). Such biases can be unintentional, for example the result of a neutral design simplification can create a persuasive bias when a particular vote is made more difficult to cast by creating an unnecessarily complex ballot.

4.1 There is single voting interface that can meet everyone's needs.

American voters make a diverse population, and thus have a diverse range of needs and preferences. Different localities may seek to place emphasis on different features of the interface, respecting the priorities of the local population and culture. The top level of the interface should be customizable, which necessitates flexibility at the lower levels to accommodate multiple interfaces. This also allows for change in the system as the needs of the community shift over time, allowing the introduction of multilingual support, for example. Within a jurisdiction, there is no need to everyone to use the same interface as long as no one is deprived their basic rights of access. The interface of voting technology should not be standardized, but rather a community should seek to ensure that everyone can cast their ballot comfortably, conveniently and with confidence. However, there are fundamental

Federal and commercial guidelines for access and usability that can guide the design of any interface.

4.2 An untrained voter should be able to know when voting equipment fails.

Just as testing and auditing help give the voter a degree of confidence about the security of the equipment and the robustness of the process, the user of a voting system should be able to know when any critical aspect of that system fails. Since the officials and vendors cannot and should not monitor every single vote, having this added degree of auditing is necessary. A controversy such as in Florida in 2000 could not have occurred if each voter knew at the time of the vote that they had marked the punchcard correctly both for the candidate and for their ballot to be read by the tallying machines. Alerts in an electronic system should consist of more than a warning light that might be overlooked, and should be integrated with voter per-vote auditing.

4.3 Access is critical: not to a specific, single technology, but to the ability to vote in a fashion that provides full civil rights.

The greatest privacy benefit of DRE voting machines accrue to those who have physical disabilities, are language minorities, and those with literacy difficulty. DRE for the first time for many of these voters allows independence in voting in public elections. However, it is not clear that everyone is best served by the same interface: if a substantial portion of the population is unfamiliar with the use of Automatic Teller Machines (ATMs) then relying on that model may alienate those voters.

Privacy has been discussed in other contexts of voting. Absentee ballots, for example, have the voter's identifying information attached as a function of their purpose. Complete anonymity is sacrificed to accommodate those who cannot make it to the polls. There are also charges that voter privacy is threatened by the use of DRE voting machines because the restricted zone around them is too small.[4] This

[4] Marcalus, Annamarie. "Mixed Reviews on Voting Electronically." Los Angeles Times, Part B; Page 70. 6 March 2004.

seems fairly easy to correct, however. When DRE's are supplemented with paper ballots, as this report suggests, then the order of anonymous ballots can be examined carefully, correlated with arrival time of any given voter to guess the vote cast by that voter.

4.4 Even with full auditing of each vote, rigorous testing for security, usability and reliability remains critical.

Security, reliability and usability are necessary for any successful voting system. Security is a measure of confidence against malicious attack, while reliability is a degree of confidence that the system will function as intended. Usability is a metric of whether the voter can cast the ballot her or she intends. None of these can ever complete, and they should not be treated as absolutes, but comparative measures: is system one more reliable than system two? Does either of them, after a year's storage, meet a minimum standard with any degree of confidence?

Testing must occur at three distinct junctures. First, the prototype model must be rigorously inspected and analyzed to make sure that it meets the original design specifications and standards and will function as intended. Second, the machines delivered to the polling places must be determined to be the same machines requisitioned, and any new software or features does not violate the original standards. Finally, the assembled and installed machines must be certified to be properly set up and calibrated, with all the functions operating as predicted.

Beyond the laboratory and polling place settings, these systems can be tested in the public by the very voters who will be using them. Colleges and high schools can use the machines for student elections, or marketing firms can deploy them in malls to gather consumer opinions. This has the combined effect of raising public awareness and familiarity with the new technology and subjecting machines to real-world stress conditions.

5. Openness of a voting process is critical for the perception of legitimacy of that process.

Openness is a democratic idea that is fitting for the foundation process of all democratic regimes. Sunshine makes the best disinfectant, and can help prevent the selection and implementation of bad or insecure systems. While openness is not a silver bullet, public confidence depends on trust in those privy to information. A process that is seen by many without protest will have a better reputation and thus may have a greater degree of legitimacy. Independent review is an important beginning, but true openness demands testing and verification for accuracy and integrity.

5.1 If underlying mechanics or software are not in the public domain, they must at least be available for inspection by the larger security community.

The greater the number of qualified experts examining a system, the greater the chance that a security flaw can be discovered. Given that determined attackers will be searching for weaknesses as well, if is in the public's interest for election officials to discover and fix security flaws first. Full public examination of the code is no guarantee of perfect security—this is impossible—but allowing the public at large to scour the code increased the likelihood that weaknesses in the code will be discovered. If the source code of the software is protected by intellectual property laws, granting access to the code is an added hassle. For this reason, among others, open source or free software may be desirable. Exposure of the underlying code serves as a further incentive for the vendors to write good code.

5.2 All security issues should be fully disclosed, although allowing vendors a limited, fixed time between notification and public disclosure could foster more public trust.

Hiding security flaws has seldom been as a robust security strategy, since "security through obscurity does not work. Security flaws should be revealed and fixed. The timing of public disclosure has been an issue of active debate in the computer security field. A short delay between discovery and exposure can encourage the vendor to fix the problem as quickly as possible, but too short a delay might not give the vendor enough time. Publication of a security flaw before widespread implementation of its solution opens the door to exploitation of the security flaw. It is ultimately the vendor's responsibility to fix security issues.

5.3 The voting technology acquisition process should be open for public scrutiny from constituents.

Just as the underlying technology should be open for criticism, so too should the process by which the technology is selected be open and public. One fear is regulatory capture, where the government officials grow too close with the voting systems vendors as their primary source of information. Officials should be forced to justify the decisions they make with respect to selecting certain technologies and rejecting others, including the initial decision to change the voting process from its current manifestation. Furthermore, openness of purchase allows individual constituencies of the decision maker to have their say, and the officials to show that they have taken these views under consideration.

5.4 The voting technology acquisition process should be open to allow jurisdictions to learn from each other. Records of difficulties should be made available to all election officials.

There is a strong tradition in information technology of "user communities" where owners and adopters of technology share information, both to help in their own experiences and to encourage common vendors to play fairly. Assessing the needs of a community and purchasing a voting machine is not a common decision for local elections officials, so it is hard for them to gain experience and acquire reputation information. All jurisdictions should try to avoid reinventing the wheel, and should learn from each other. This can prevent bad decisions and vendor deception.

6. Election systems must have built-in auditing capability.

A certified election asserts that the vote that was counted is the same vote that was cast by the voter. As such, if there is any question about the execution of an election, the results must be examined for a verified account of the election. This auditing process needs to be informed by the underlying technology, but all audits have must have certain properties. An audit includes a recount of the ballots, but can also involve an examination of the systems used, the process of the election and the possession and treatment of the ballots. A DRE system with no physical record of individual votes cannot meet these criteria.

6.1 The reconciliation process must be clear, precise, authoritative and binding.

To be clear, the general public must understand what is going on, and exactly what will be ascertained by an audit. This includes an awareness of what will and will not be verified by the audit. The process derives its authority by being designed and subject to scrutiny before the election. It must be designed to confer legitimacy on the results, and should be acknowledged by all parties. A binding reconciliation process should not be open to direct challenges. That is, concerned parties should only be able to argue that it was not executed properly, not that the auditing plan itself was flawed. Clarity, precision, authority and binding reconciliation ensure that the process by which questions about the election are answered gives credibility to those answers.

6.2 The cast ballot must follow a "Chain of custody" from the moment it is cast to the moment the vote is entered into the final official tally.

The chain of custody must be subject to audit and oversight at each step regardless of technology. The nature of the audit and oversight may be specified based on the technology.

Throughout this process, no one actor should be able to secretly destroy or alter ballots. Partisan competition and dual-party monitoring can be used as safeguards. Each ballot must be accounted for, which may necessitate records kept at the polling place of how many blank ballots were used, and record their entry into the tally. It is important to also respect the anonymous nature of each ballot in this process. Each voting jurisdiction must make adequate preparations for an audit for each election, so adequate numbers of officials, observers and law enforcement are available if needed. The myriad of issues that can arise in the auditing process should be part of election officials' contingency plans.

6.3 If some metric of voting irregularity is exceeded in a given jurisdiction, a court-supervised manual recount should be required.

Many voting irregularities can be traced back to flaws in the voting systems. Any recount that is concerned with error introduced by the voting systems themselves should deal with the paper ballots, particularly voter-verified paper ballots. Triggering an automatic audit at a certain threshold does not preclude audits from occurring at other times, but saves the trouble of argument in obviously close or questionable elections.

6.4 Auditing should not be implemented by a vendor affiliated with the original system.

In the event that the election officials turn to the private sector to aid in the auditing process, the standard industry practice must be used for securing and independent, third-party system. The purpose is to examine the entire system, not just the votes, so having an outsider view the technology can help guarantee a less opportunity and motivation for bias. Open systems make this process more straightforward.

6.5 Equipment testing does not displace the need for outcome auditing.

Testing is necessary but not sufficient for a well-run election. Testing is never perfect, as it can overlook certain factors or interactions which may be easier to detect in hindsight. Systems interact with each other in unpredictable ways, often impossible to detect in a reasonable battery of tests. It is also harder to examine the human element discussed above. Outcome auditing can also confirm the validity of testing for future elections although, again, it is no guarantee.