AUDITABILITY OF NON-BALLOT, POLL-SITE VOTING SYSTEMS

by
Roy G. Saltman, M.S., M.P.A.
Consultant on Election Policy and Technology
rsaltman@alum.mit.edu
Revised: August 24, 2003

Abstract

The history of the use of non-ballot voting systems in the US is briefly described. The background of a current controversy is also noted. The differences between DREs as currently used and Internet voting are discussed. The voting process as a human system involving people, procedures and activities as well as machines is stressed. Alternative systems employing ballots are described, and their advantages and disadvantages as compared to DREs are discussed. Specific machine design changes and administrative changes in the testing and use of DREs are recommended.

1. Background

The question of implementation of audit trails in non-ballot, i.e., direct-recording electronic (DRE) voting systems, is not new. It was discussed extensively in 1988 [Saltman, R., 1988, pp. 40, 41, 112-114] and a requirement for part of the recommendations proposed in 1988 was included in the Federal Election Commission standards of 1990 [Federal Election Commission, 1990, p. 18]. Recently, the topic arose again in connection with the desire of officials of Santa Clara County, California, to procure DRE systems for use by the voters of that county. Opponents of this procurement, led by David Dill, professor of computer science at Stanford University, proposed a requirement for a paper audit trail that is "voter verified." That is, a paper record of the ballot would need to be produced by the DRE voting unit and approved by each voter before the ballot is cast. This demand of Dill and other computer scientists follows the recommendation of Rebecca Mercuri, professor of computer science at Bryn Mawr College, that has been presented on several occasions [e.g., Mercuri, R., Neumann, P., 2003, p. 40].

Following a request by officials of Santa Clara County for an opinion from the state, the Office of the Secretary of State of California undertook a study and issued a report [Secretary of State's Ad Hoc Touch Screen Task Force, 2003]. The Task Force made several recommendations to improve the security and integrity of voting systems, and noted the new federal requirement that there must be a paper record for each ballot cast. The federal statute is interpreted to mean that the individual records could be printed in bulk from electronic records after the polls are closed. However, the Task Force stated:

> "For technical and logistical reasons there is no support to have the printing of this permanent paper record done at the time the ballot is cast ..."

Thus, the state did not accept the demand of the computer scientists, but allowed that a county could purchase systems with this feature, if it so chose. The purpose of the discussion below is to further elaborate the arguments on both sides and to consider improved mechanisms that would increase voter confidence in the results produced by DRE voting machines.

2. Lever Machines:

The use of non-ballot, poll-site voting systems in the US goes back over one-hundred years. In 1899, the US Congress approved the use of non-ballot mechanical lever machines in voting for candidates for the US House of Representatives. After that, the use of lever machines spread widely and, for the general election of 1960, the last Presidential election before the start of adoption of punch-card voting, it was reported that 55 % to 60% of the voters in this nation used them. In the Presidential election of 2000, they were used by about 19 % of US voters. Interestingly, no concerted effort by computer scientists was ever mounted, in the roughly forty years that computer science has been a profession, to persuade election officials not to use lever machines, despite their clear failure to provide an audit trail. This writer, however, has discussed the difficulties of these machines [Saltman, R., 1988, pp. 26-29].

The complete auditability of mechanical lever machines is not possible. Individual voter-choice sets, i.e., the groups of particular votes cast for all contests by each individual voter, are not retained. Consequently, there can be no demonstration of the complete content of any voter's set of selections. Only the sums of votes cast by all voters for each candidate and issue alternative are stored. As a result, it is not possible to determine the cause of a vote recorded as not cast in a contest without a close examination of the internal workings of the particular machine that was used. It may be that a voter chose not to cast the vote in question, but it may be that the voter attempted to cast it but the machine, because of an internal malfunction, failed to record it. (The machine failure may have been due to a structural defect that gradually appeared without being noticed on account of a lack of adequate maintenance, but it is possible that the malfunction was due to malicious human action.)

3. DREs:

These machines began to be used in1974. An experimental model was referred to in a report in 1975 as an "electronic vote summarizer" [Saltman, R., 1975, p. 13, 14]. There are three basic types used in the United States: pushbutton, micro-switch and touchscreen. The first DREs used pushbuttons to replace the levers. The next improvement was the use of micro-switches, activated by voter touch, placed beneath a hard but somewhat flexible surface on which the choices were presented. The newest development involves the presentation of candidates' names on an electronic monitor within areas of the screen sensitized to touch. A touch of the screen at the location in which a candidate's name is presented causes the computer to respond programmatically. All three of these types continue to be used. DREs became popular slowly; in 1988, they were used by only 2.7 % of the US electorate, but in 2000, 10 % of all voters used them. As a result of the debacle of punch card voting in the 2000 Presidential election in Florida and the subsequent passage of the (Federal) Help America Vote Act (HAVA), their usage is likely to increase significantly. For example, Georgia used them throughout the state in 2002. Maryland has decreed that any of its 23 counties that are not using them now will eventually use them at poll sites; mark-sense ballots will be used for absentee voting. Baltimore city, Montgomery County and Prince Georges County, three of Maryland's most heavily populated jurisdictions, used DREs in 2002.

Since the specification of the 1990 Federal Election Commission standards that "electronic ballot

images" (their phraseology for "voter-choice sets") be retained within the machines, it is very likely that all DREs produced since then have this capability. Additional design features should be mandated, and additional testing and system assurance operations should similarly be required. These concerns are addressed below.

4. <u>Voting Over the Internet:</u>

This presentation does not concern voting over the Internet. It concerns only poll-site voting; that is, voting in which individual votes are **not** communicated electronically outside of the physical location in which they are cast in order to be summarized with other votes for the same candidate. Internet voting involves additional levels of risk and additional controls beyond the scope of this paper. The risks of Internet voting should not be used to taint the use of DREs by combining the latter with the former as "electronic voting" and by giving the impression that the unique difficulties of Internet voting apply also to DREs. There is no reason for DREs to use the Internet during operations, and those recently purchased for Maryland will not do so, despite the implication to the contrary in a recent study [Kohno, T., Rubin, A. et al, 2003]. That study also attempted to analyze DRE software separated from the election system of which it apart - a fatal error. See **Section 5** about the systems concept.

5. <u>Voting as a Human System:</u>

It must be understood that voting is a complex system involving people as well as machines. Concerns for the system cannot be reduced to the single issue of correctness of software, although that is certainly important. Information systems used by both business and government are tools that people use to assist them in performing their duties and achieving results defined by organizational management. Some of the criteria for success of the particularly complex system for voting are these: (1) the voters are easily able to convert their choices exactly as they intend into commands to the system; (2) the system processes the voters' choices correctly; and (3) there is public confidence in the results produced by the system. Mistakes can be made, and often the mistakes are made by people - the voters or the administrators.

The integrity of the information system for voting involves considerably more that just correctness of software. The latter issue as the only essential one was first raised in *The Los Angeles Times* in 1969 and in *The New York Times* in 1985. The story made the front pages of major newspapers twice because the idea of software manipulation was sensationalistic. The presentations' positive value was that they sensitized policy makers to the potential threats to administration of elections and generated studies on the reductions of threats. The negative value of the stories was that the special focus detracted from the necessary view of how to improve the entire process from a systems perspective.

In 1989, I was asked by the International Association of Clerks, Recorders, Election Officials and Treasurers (IACREOT) to present, at their annual meeting that year in San Diego, my answers to three specific questions. The first of the questions was the following:

> What ways are there that would make it possible to "rig" an election using computers, i.e., Voting Machines, Direct Electronic Voting, Punchcard and Optical

Scan Equipment? [Saltman, R., 1989, p. 1]

My response continues to be pertinent, because the same question constantly arises in essentially the same context. Here is part of my answer:

> "Election administration is a **system** that consists of four elements: (1) people, (2) established procedures, (3) devices and machines, and (4) activities. Election administration activities should be undertaken, according to established procedures, by the people using the devices and machines. Before there were computers, there were other devices and machines used in election administration and, consequently, some procedures were different.
>
> "However, the election administration process was a **system** then; it remains a **system** now. The use of computers has not changed that. The process remains a system that is managed and carried out by people, that is, election administrators. Election administrators, not vendors, not manufacturers, not other contractors, are responsible for the accuracy of the results produced, in order to assure that the "consent of the governed" is truly achieved.
>
> "The reason that I have stressed that election administration is a system is that **it is not possible to separate the question of manipulation of computers for election "rigging" from considerations of the system of which the computer is a part.** If a computer has been used to "rig" an election, either the procedures used to carry out the election were inadequate, or the people managing and carrying out the activities did not follow established procedures. Thus, instead of telling you what ways there are to use a computer to "rig" an election, I must tell you what proper and effective procedures there are, to be used by you, the election administrators, to assure accurate results that correctly reveal the choices of the voters.
>
> "These proper and effective procedures need to include those used to (1) **acquire** hardware and software according to performance specifications, (2) **check out** hardware and software for logical correctness, integrity and reliability, (3) **protect** acquired hardware and software against unauthorized access, and (4) **effectively employ** hardware and software in election operations."

6. <u>Vulnerabilities of Ballot Systems:</u>

<u>Ballot-counting voting systems</u> are not necessarily less vulnerable to mistakes and fraud than non-ballot systems. In fact, one of the major reasons that mechanical lever machines were adopted in the US in the early 20th century was because of significant ballot frauds. Two vulnerabilities of these systems are:

(1) **Ballot-readers are not totally accurate**, particularly when attempting to read marks or punches made by real humans. The difficulties in punch card systems need not be elaborated; they are too well known. Voters using mark-sense systems may make marks that are too light to be accurately sensed, may make smudges at unintended voting positions that may be sensed by mistake or may use

an incorrect writing instrument that fails to register their votes. They may make marks outside of the assigned areas that the machine can sense, requiring an "intent of the voter" manual analysis. Furthermore, mark-sense readers may be reduced in sensitivity by dust from ballots or from the environment.

(2) **Ballots may be miscounted,** even if there is no ballot-stuffing. In Florida, in the 2000 Presidential election, several counties using ballot-counting systems found significant numbers of additional ballots in their automatic machine recounts. In one county, a poll station manager, with the ballot cards in the trunk of her car, stopped off to see a friend before delivering the ballots and forgot about them. Nassau County's recount was different (adding a net 71 votes for Gore) than its original count, but the County Canvassing Board decided that their first count was correct, not their second one. As a result, Gore's contest of the certified vote count separately included a demand for another recount in Nassau County. When the US Supreme Court summarily and prematurely ended the statewide recount ordered by the Florida Supreme Court, a result was that a true determination of the Nassau County results was never completed.

7. <u>Vulnerabilities of DREs:</u>

DRE counting systems have the vulnerability that there is no hard-copy audit trail. It is important to note that a hard-copy ballot, created by a programmed computer even if the input is provided by the voter, does not automatically constitute a document-ballot that is independent of the computing machinery. As I stated in 1988, "the fact that the voter can see his or choices on a display, or even receives a printout of the choices made, does not prove that those were the choices actually recorded in the machine to be summarized for generating the results of the election" [Saltman, R., 1988, p. 41]. **A printout or hard-copy ballot produced by the machine is not independently created by the voter; it is subject to the correctness or incorrectness of the computer program that created it.** With electronic non-ballot voting systems, the computer program actually casts the votes. The computer may cast votes that differ from the voter's intent if the program was written to carry out that insidiously incorrect activity [Saltman, R., 2003, p. 133].

8. <u>Value of a Printout for DREs:</u>

If the intention of a printout from a DRE machine is to give the voter a sense of confidence that his or her vote was properly cast and properly processed, that confidence would be false. Due to the fact that the printout is created by the computer and is not a document-ballot, such a printout is a sop to the layperson ignorant of the inner workings of computers. There must be better ways of providing the necessary confidence to the voters. It is the intention of this paper to propose some.

9. <u>The Ballot Solution to the DRE Auditability Problem:</u>

A DRE voting unit may be considered as three subunits. The first subunit may be called the Vote-Entry Section (VES) and the second subunit may be called the Vote-Summarizing Section (VSS). The input to the VES are the voter's choices, typically entered through the voter's fingers acting on pushbuttons, micro-switches, a keyboard, a mouse or a touchscreen, and its outputs are the voter's choices converted to an electronic form (voter's electronic ballot image or EBI). The inputs to the VSS are the outputs from the VES for each voter, and the output of the VSS is the summary of votes cast on the DRE. The third subunit, the Ballot Image Storage Unit (BISU) also receives the

EBIs from the VES and permanently stores them in a secure manner so that they cannot be overridden.

Suppose that the VSS were separated from the other two subunits, but was still in the same physical location, so that the output of the VES would not go directly to the VSS, but instead would go to a printer that would generate a mark-sense ballot. The mark-sense ballot could be created in a language of the voter's choosing, assuming the language were pre-programmed, meeting the multi-language requirements of the Voting Rights Act. This mark-sense ballot, because it would be machine-generated, would have a very high likelihood of being read correctly by a mark-sense reader. Suppose, then, that the voter had the opportunity to review the mark-sense ballot and found it to mirror exactly what the voter intended. Then the voter could deposit the mark-sense ballot in an **independently programmed** VSS through a mark-sense ballot reader. Then, if "the cast ballot becomes the only source of vote-recording and counting, it would be considered a document-ballot. Then the voting system would not be a non-ballot system" [Saltman, R., 2003, p. 133].

A system such as this has been proposed by Alan Dechert for use in California. This type of system would be acceptable to those demanding a "voter verified" audit trail. It is not a DRE system. Is it still possible, with additional controls designed into the machine and the system, to allow for the use of a DRE with confidence that it is providing the correct results? Consider the following recommendations.

10. The Human System Solution to the DRE Auditability Problem:

The ballot solution presented above eliminates the "intent of the voter" issue because of the machine-generated ballots, However, it includes an extra printer for each VES and an extra ballot-reader for each VSS. It negates also the value of a DRE because it uses paper ballots. Recent studies of the economics of different system types demonstrate that the cost of paper ballots that cannot be re-used is significant. That is, the operational cost of a ballot-using system must include the paper ballots for each election, a cost that does not have to be borne by DRE systems. The operational cost of ballots may, over time, cause total system costs of ballot systems to be greater than that of DRE systems.

10.1 The DRE Design Part of the Solution: If DRE systems are to be used without the production of hard-copy ballots, the problem of an audit trail that can be trusted must be solved. The following design features are recommended. They are specifically proposed with a view toward improving human factors and increasing public confidence in the results produced by the system. Whether or not the proposed features make the DRE acceptable is a decision to be made by the elected political leaders of the jurisdiction purchasing the voting system.

(1) **Resetting of each machine following the completion of each voter's effort:** Each completion of the voting process by a voter should result in the machine's inability to receive any more commands until reset for the next voter. It is likely that this activity is now being carried out with most DRE systems, but is restated here because of the claim of the study by Kohno, Rubin et al. that implied that one voter could continually use the machine to insert many votes.

(2) **Direct report to the voter on his or her contribution to the count of votes:** A significant concern of computer scientists appears to be the inability of the voter to discern the fact that his or her vote was counted. With the use of precinct-located mark-sense ballot systems, when the voter deposits his or her ballot in the reader, a counter on the machine visible to the voter will increase by "one," demonstrating to the voter that the ballot was added to the pile of ballots already received. In that system, the voter has no information as to what happens to the ballot after it is deposited. It may be maliciously altered or replaced by a counterfeit, but the fact that the count of ballots is increased by "one" seems to be satisfactory to the computer scientists who claim to know what constitutes voter confidence. Therefore, it is proposed that the DRE machine, as a result of the voter reporting "all voting complete," should present a final screen showing to the voter the previous number of votes received by the machine and that number increased by "one." That action will demonstrate to the voter that his or her votes were added to those already received.

(3) **Recording of EBIs and recounting on a separately programmed machine:** DRE machines provide for the retention of EBIs in the BISU. The recording should be on a removable diskette that can be inserted in a separate independently programmed machine for recounting. Thus, California's requirement that one-percent of the precincts be recounted could be met. The retention of the EBIs allows also for their printout to meet the new HAVA requirement.

(4) **Reconciliation of all votes and undervotes:** All undervotes should be positively recorded for purposes of reconciliation. (Overvotes are not possible on a DRE). This is not done now, but I previously recommended it [Saltman, R., 1988, p. 112, 113]. Reconciliation should be accomplished by designing into the internal logic of each VES, a special "no-vote" bit for each contest. (We assume, for simplicity, only 'vote-for-one' contests. The solution is easily extended to 'vote-for-N' situations.) In typical current systems, there is, in the VES internal logic, a "vote" bit for each candidate that is set to "zero" when the machine is activated for a new voter. When a voter selects a candidate, the "vote" bit for that candidate is set to "one." If the voter fails to vote in the contest, no bit is set to "one" in the voter's EBI, and when the voter is finished voting, no "one" bit is recorded or transmitted to the VSS for that contest.

As proposed here, each contest would have, in addition to a "vote" bit for each candidate, a single "no-vote" bit which would be set to "one" when the VES is reset for a new voter. If the voter votes in the contest for any candidate, the "no-vote" bit is reset to "zero." If the voter has completed the voting process and has not voted in a contest, the value of the "no-vote" bit, which should still be a "one" is transmitted to the VSS in the voter's EBI. This process provides for the transmission of one "one" for every 'vote-for-one' contest and provides that the number of "ones" in each EBI sums to the number of vote-for-one contests on the ballot. It also allows for the use of an additional results line that specifies the number of "no-votes" for each contest. The reconciliation occurs in that, for the results of every contest, the sum of the number of votes for candidates plus the number of "no-votes" always equals the number of voters that have used the machine. The number of votes not cast in each contest should be printed, along with the votes cast for each candidate or issue alternative. This reconciliation is intended to further public confidence in the results.

(5) **Second-chance voting:** The addition of the "no-vote" bit for each contest in the VES provides

the information to allow the machine to report to the voter, if the "all voting complete" indicator has been prematurely activated, that the voter has not voted all contests. In a touchscreen system, the information available will allow the machine to report on the screen the highest contest not yet voted, and should allow the voter to continue voting, if that is desired. This is of particular value to the voter if the voter has mistakenly activated the "all voting complete" indicator too early as an unintended reflex action. In the use of Internet web sites or with application programs, many systems will respond to a user who mistakenly activates a command with a screen or display that permits the user to retract the command, e.g., with a "cancel" option. Election administrators should do no less for voters.

(6) **Voter's review of choices:** The DRE should be designed so that the voter may review choices in each contest before completing the voting process. With a full-face DRE, the voter needs only to look at the choices clearly presented in front of him or her. With a monitor screen, the voter needs to be able to return to the screen for any contest. The capability to do that must be clearly shown to the voter. Human-factors research could investigate the best manner to show the summary of choices to the voter. The demand that this information should be on paper rather than just on the full-face DRE or on a computer monitor is puzzling. It harks back to the time when computers first began to be used in the 1950s and 1960s, and skeptics re-calculated results on electro-mechanical machines because they did not trust the computer. Now we have better methods of assuring software correctness.

(7) **Naming of the "All Voting Complete" indicator:** This indicator should not be called "Vote." That name is confusing in its similarity with the completion of action on a particular contest. A more definitive name such as "All Voting Complete" needs to be used.

(8) **Connector for entry of test votes:** There should be a physical connector on the VES which allows for entry of a series of electronic test votes of any number, as if many voters had voted on the machine. The entry point should replace the voter inputs that would fill the temporary storage location with voter's selections in the VES, so that the recording of the selections in the BISU and the summarization process of the VSS may be checked. I have seen a device that generates test votes and exercises a DRE through a connector, as I have proposed. Thus, it has already been done for at least one system. Note that the testing will not test the correctness, in the VES, of the transference of the voter's choices to the temporary storage locations in which the choices are first stored. This part of the VES would need to be separately checked.

10.2 The Software and Hardware Assurance Part of the Solution: All software and hardware to be used must be thoroughly checked out upon delivery following procurement, and then again in preparation for any election. As the integrity of elections using DRE equipment depends on software and hardware correctness, testing must be thorough. Software should be required to be written so that, in preparation for any election, the logic of the software remains unchanged and only blanks are filled in to adapt or specialize the software for a particular election. Software testing must assure the lack of hidden loops that are intended to be exercised only at a particular time or only when a particular value is inserted in a specialization process. My reports of 1975 and 1988 are filled with recommendations of procedures for carrying out systems assurance.

10.3 Audit Trail for Software Handling: It is essential that specifications be written and followed as to the manner in which all software and storage units containing software are to be handled, tested and transported to assure integrity. That is, an audit trail needs to be established for the handling of software. These procedures, if well written and carried out, will prevent the rumors of software manipulation that flourish in an atmosphere of lack of knowledge and lack of specificity.

10.4 The Administrative Implementation of Assurance: It is desirable that each state establish its own system integrity process beyond that established through the NASED-sponsored Independent Testing Authorities. Additional testing may need to be provided. Each state may wish, further, to establish a Voting System Assurance Advisory Committee, with a Computer Technology Subcommittee, that will recommend system assurance procedures. The latter group should be able to help devise the best methods for testing of software to assure correctness and the absence of malicious code. The establishment of these administrative structures and the publication, for public dissemination, of what is being done, will provide the public confidence in the operation of elections that is currently lacking.

11. Summary:

Possible changes in the design of DRE units and the administration of the vote-counting system have been proposed. The intention of these proposed changes is to improve the auditability of DRE systems and thereby to improve public confidence in the results produced. An alternative ballot-counting system has been discussed, and its differences with DRE systems have been noted.

The assurance of public confidence in vote-counting is an issue of systems design and assurance; it is not limited to a single palliative measure, e.g., the provision of hard-copy ballots in DRE systems. Assurance of public confidence is not a new issue. For example, my 1975 report contains the following:

> "The assurance that steps are being taken by election officials to prevent unauthorized computer program alteration or other computer-related manipulations remains, nationwide, a continuing problem for the maintenance of public confidence in the election process" [Saltman, R., 1975, p. 4].

The solution to the issue of public confidence requires reviewing the vote-counting information system from a multi-disciplinary perspective. Public administration, human factors concepts, information systems engineering, internal auditing, public communications, and other disciplines are important to apply, as well as computer science.

12. References:

Federal Election Commission, 1990, Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems, Washington, DC.

Mercuri, R., Neumann, P., 2003, "Verification For Electronic Balloting Systems," in Gritzalis, D.

(ed.), Secure Electronic Voting, Kluwer Academic Publishers, Boston, MA.

Kohno, T., Rubin, A., Stubblefield, A., Wallach, D., 2003, Analysis of an Electronic Voting System, Information Security Institute, Johns Hopkins University, Baltimore, MD.

Saltman, R., 1975, Effective Use of Computing Technology in Vote-Tallying, NBSIR 75-687, March, 1975 (reprinted as NBS SP 500-30, April, 1978), National Bureau of Standards, Washington, DC (now National Institute of Standards and Technology, Gaithersburg, MD).

Saltman, R., 1988, Accuracy, Integrity, and Security in Computerized Vote-Tallying, NBS Special Publication 500-158, National Bureau of Standards, Gaithersburg, MD, (now National Institute of Standards and Technology, Gaithersburg, MD).

Saltman, R., 1989, Accuracy and Integrity of Computerized Vote-Counting: Answers to Three Fundamental Questions Posed by Election Administrators, Presentation to IACREOT annual meeting, San Diego, CA, June, 1989.

Saltman, R., 2003, "Public Confidence and Auditability in Voting Systems," in Gritzalis, D., (ed.), Secure Electronic Voting, Kluwer Academic Publishers, Boston, MA.