Fair, Accurate, and Accountable Voting Systems

John Baldwin, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, jbaldwin@uic.edu

Sharon Baldwin, Baldwin919@aol.com

Marco Mazzucco, Laboratory for Advanced Computing, University of Illinois at Chicago, marco@dmg.org

Foundations of Electronic Government in America's Cities: A Multi-Disciplinary Workshop

March 8 & 9, 2001

Chicago, IL

Abstract: The2000 election raised serious accuracy and/or security concerns with all current voting systems. After examining these problems we describe criteria any system should meet. We propose a protocol which is technically feasible *now* and which meets these criteria.

Most voters have trusted that the systems provided for casting their votes actually produce a reliable and precise record of the votes cast. The Florida election fiasco of 2000 has jolted that complacency. The difference in the number of votes cast for Bush and Gore was less than the margin of error of the system used for casting and counting the ballots, and there was no simple, quick and evenhanded solution available to eliminate that error. The importance of the election publicized the existence of this margin of error, which varied significantly among different voting systems and among different groups of voters. Election professionals have always been aware that there was a margin of error in each system; there are always votes that for one reason or another are not counted. This error was considered relatively unimportant and easily outweighed by considerations of convenience and cost, because it was generally assumed that the error rate would rarely affect the outcome, that the error was random among groups of voters, and that the rate could be reduced by manual recounts where needed. Election 2000 has shown that these are unwarranted assumptions, and underlined the need for a better system. The popular punch-card system received the worst press of the systems used in Florida, but certain implementations of the modern optical scanner system had the worst problems[1]. Technologically unsophisticated and elderly voters proved to be at greatest risk for having their votes rejected.

The disagreement between Renquist's concurrence in Bush v. Gore and the Florida Supreme Court opinion spotlights the weakness in current systems. Justice

Rehnquist argued that it was absurd to believe that the Florida legislature had enacted a scheme “in which machines are required to be `capable of counting correct votes’ but which nonetheless regularly produces results in which legal votes are predictably *not* tabulated, so that in close elections manual recounts are regularly required.”[i] The Florida Supreme Court, with a more realistic or cynical view of what it means for a machine to be capable of counting correct votes, wrote that “The issue in dispute here is the meaning of the phrase `error in the vote tabulation’ found in section 102.166(5). The Division [of Elections] opines that the phrase `error in the vote tabulation’ only means a counting error resulting from incorrect election parameters or errors in the vote tabulating software. We disagree. The plain language of section 102.166(5) refers to an error in the vote tabulation not the vote tabulation system. On its face, the statute does not include any words of limitation; rather it provides a remedy for any type of mistake in tabulating ballots.”[ii] Regardless of which interpretation fit the facts in the year 2000, we intend to describe a voting system that makes Justice Rehnquist’s dream come true: a system where the `ballot-record’ so accurately reflects the voters intent that a manual recount is required only in the case of fraud or unpredictable machine malfunction and which improves the reliability of this recount.

This article focuses on improving fairness and accuracy of elections as currently held: almost all voters cast their ballots at polling places on the same day . Issues raised by trends toward advance voting, the vast increase in absentee ballots (up to 1/3 of the ballots cast in some states), and the possibility of internet voting all raise fundamental questions outside the scope of this paper. The Workshop on Internet

Voting (October 2000) found: "Pollsite internet voting systems offer some benefits and could be responsibly fielded with in the next several election cycles. ... Remote internet voting systems pose significant risk to the integrity of the voting process and should not be fielded for use in public elections until substantial technical and social issues are addressed."[iii] In line with that report this paper focuses on protocols for systems which could be deployed in the immediate future. We begin by describing criteria for a voting system. We then describe how the current systems in the United States fail these criteria. We sketch a feasible and even affordable electronic voting protocol which meets the requirements.

Section 1: Criteria. There are three steps in the voting process: determining who is eligible to vote, casting the votes, and counting the votes. Eligibility is not discussed here; we describe separately the criteria for `vote casting' and `vote tallying', followed by some overall considerations.

I. Vote Casting

A. The voter should be able to easily and clearly express his intent.

B. The voter should be able to easily check that his intent has been expressed and correct or exchange his ballot if it has not.

Currently, many voters make unknowing errors; thus, a system that does not permit over- or under-votes provides a definite advantage. Even the voter who realizes he has made an error on his ballot may be reluctant (perhaps because of time pressure or embarassment) to ask that it be spoiled and a new ballot issued. Such corrections should be possible with minimal intervention by election personnel. The ability (mandated by a Cook County Circuit Court ruling in January) to check a punch card ballot and correct over- or under-votes reduced the number of spoiled ballots in the 37th ward of Chicago from 12.4 per cent in the presidential election (checking not permitted) to slightly over 1 per cent in the special aldermanic election in March 2001.[iv]

C. There should be no way to identify the ballot of any voter.

The importance of the secret ballot in preventing the sale of votes and intimidation of voters does not even require discussion. Thus, there should be *no* interaction between the system of voter registration determining eligibility to vote and the systems for recording and counting votes; they should be on distinct computer systems.

II. Vote tallying

A. There should be a rapid and accurate method of tallying the votes.
B. There should be an audit trail available to permit any inaccuracies of the original tally to be corrected.

Ideally, an audit trail is an unambiguous list of the votes cast at each precinct, which can be retallied to check for errors. As Michael Shamos pointed out[v], no system providing such an *unambiguous* list has been devised. The aim must be a record that will disclose any actual fraud or serious misrepresentation of the vote and maximize the ability to reconstruct the intended votes. Historically, such an audit trail has been a physical collection of ballots, which could be recounted by hand. The election of 2000 and its aftermath have shown the difficulty of relying on manual recounts.

III. General Considerations

A. The system should be as tamper-proof as possible.
B. The system should be uniform across the jurisdiction.

The Supreme Court in *Bush v. Gore* found [vi] that the failure of the Florida Supreme

Court to clarify the `voter intent' standard by specific criteria for evaluating disputed ballots violated the equal protection clause. Whether permitting local election authorities to use different systems with different degrees of accuracy also violates equal protection was not before the courts this year. It is at least arguable that the use of different voting systems in different parts of a state with ballot rejection rates ranging from .003 to .17 (as opposed to the approximately .005 in counties with the most controversy which were subject to the different standards cited by the court) constitutes a similar violation of equal protection. Startlingly, the probability of the voter s intent not being properly tabulated by the voting system was up to 50 times greater in various precincts in Atlanta which rejected 1/6 of the ballots[vii] than under optical scanner or electronic voting systems which rejected less than 1/3 of one percent of the ballots.

Whether or not it is constitutionally required, simple fairness and a desire to maintain confidence in the electoral system require a more uniform voting system. The same principles of fairness that underlie the necessity for uniform methods of verifying the vote tabulation (the “pregnant chad” problem) support the use of statewide requirements so that a vote in one county is as likely to be counted accurately as in another county. Rather than a mandate of a specific system, state certification of various systems is desirable. No system that on a regular basis rejects more of 1% of the ballots for the highest office contested should be permitted.

C. Costs should be minimized.

Section 2: Current systems: Each of paper ballots, lever voting machines, punch cards, optical scanners and electronic systems fail some of these critera.

Paper Ballot: In the United States, where both the number of offices elected and the number of voters are large, hand-counted paper ballots are impractical.

Lever voting machines: The Florida punch card problems have raised nostalgic memories of the lever voting machines of the 60's that at least made overvotes impossible. But these machines were abandoned in most jurisdictions because of their maintenance cost and security problems. Both the voting mechanisms (put gum under the `Bush' handle) and the tally mechanism are insecure. There is no audit trail that permits reconstruction of the vote. Instead of a record of votes, there are only cumulative totals for the day. It is usually possible to determine if tampering altered the count, but there is no means of recovering any approximation of the actual vote.

Punch card voting: Punch card systems do not provide an easy and accurate record of voter intent. First, the voter has to be familiar with the punch card technology even to be aware that the ballot should be checked to ensure that the proper holes, and only the proper holes, have been punched out. Second, the time involved in checking whether the correct hole has been punched in each race is prohibitive. (The voter in Cook County may have as many as 100 different choices to record.) One cannot easily correct a punch card as any error requires spoiling that ballot and starting all over. An unsophisticated voter (especially one who grew up with the voting machine which permitted corrections) may think that pressing a second candidate automatically corrects a previous press for another candidate.

Nor do punch card systems provide an accurate tally; they routinely fail to count 2 per cent of the ballots. This figure increases in some jurisdictions to 10 per cent or even 1/6 of the ballots[viiii]. The `undercount' is not random but is higher among minority and low income voters. Further, the error rate is increasing. In Chicago, the presidential undervote increased from 3.2 per cent in 1992 to 3.7 per cent in 1996 to 7.1% in 2000 (there was a much smaller increase statewide). The reason for this increase is not known; contributing factors may include deteriorating equipment and the abolition of straight-ticket voting. Punch cards are significantly less accurate than voting machines in many jurisdictions (E.g. in certain (Democratic) downstate-Illinois counties 2.2 per cent of the vote was undercounted by voting machines and 5.8 per cent in the first election with punch cards.[ix]) These problems are caused by difficulty in aligning punch cards in the template, improperly prepared cards (making chads too easy (fostering double votes) or too hard (undervotes) to remove), and confusing ballot design (*passe* Palm Beach and the Chicago judicial ballot). The "butterfly ballot" not only confused the voters but was criticized by the inventor of the Voto-matic system as putting the holes in the ballot too close together and causing the machine to jam. Further, the tallying of punch cards is affected by heat, humidity, and wear on the card from repeated counts. Thus, while a system permitting a punch card to be checked by the voter before it is deposited in the ballot box would lower the error rate, it would not eliminate uncounted ballots.

Optical Scanning: Optical scanners are generally more accurate than punch cards. Brooks Jackson of CNN reported on Nov. 30, 2000 that CNN had done its own calculations and had discovered that "[t]hirty-six Florida counties that use optical scanners recorded an average undervote of just over .03 percent [by CNN's figures], while 18 counties using punch-card systems reported an undercount of more than 1.5 percent --a substantial disparity."[ix] But the overvote on scanning systems could also have altered the outcome. The Orlando Sentinel [xi] found 3114 overvoted ballots in Lake County, Florida (more than 3 per cent of the county vote) that had been discarded by the optical scanner. On 622 of these ballots (more than 1/2% of the county vote), the voter had both marked a listed candidate line and had written in the name of that same candidate. On these uncounted ballots, 246 voters had written in votes for Bush, 376 for Gore. As the county-wide totals ran 3 to 2 for Bush, the Lake County errors were not random among voters; the errors in Lake county were 1/4 of the statewide margin. An investigation by the Chicago Tribune and Orlando-Sun Sentinel revealed that the greatest number of spoiled ballots in Florida occurred in the 15 counties where paper ballots were tabulated by centrally located optical scanning equipment. There was a 5.7 per cent spoiled ballot (over or under-vote) rate in those counties compared to   3.9 per cent in the punch card counties. The investigation found that of the 15, 596 rejected ballots, 1776 showed a clear choice (with a gain of 336 votes for Gore). Another 5002 ballots rejected in these counties had discernible votes (with a gain of 944 votes for Gore). These ballots suffered from defects in design (2 columns encouraged double vote for president) or several voter marks for the same candidate. In short the ability of the voter to confirm his choice is crucial.[1]

Electronic voting: We call a system electronic if it provides direct record entry (DRE) of votes onto electronic media. We list principles for the design of such systems which, if

[1] Chicago Tribune, January 28, 2001

observed, would meet the goal. *Most existing systems do not meet these criteria*.

Principles for the design of an electronic voting system include the following:

1. The registration, vote casting, and vote tallying systems shall be completely separate; they must run on different machines.
2. Vote casting is on dedicated stand-alone units; results should be recorded on write-once media, which are physically delivered to a central tallying unit.
3. The order in which votes are cast is not reflected in their order on the media nor by any time stamp.
4. Ballot configuration is by election personnel, on election board machines.
5. Vote tallying is by election personnel, on election board machines.
6. Software is open source.

If the three parts of the voting system are kept rigorously apart, electronic registration and tallying present no *new* security concerns. Vote casting is different. The computer produces a record supposedly of the votes cast during the day. Through appropriate cryptography that record can be made more secure against hacking than physical ballots can be made against tampering, theft, and ballot box stuffing. The step between what the voter sees on the screen and what is actually recorded, however, is vulnerable. The unit should be designed so that the only inputs it can accept are the setting of the election parameters (by a suitably identified official) and registering of ballots. When the polls close, the media is removed and set to receive no further data. Nevertheless, the possibility of program error or malicious programming is severe. Running the program on various test data provides the only protections against such difficulties. (See Shamos[xii].) In addition to actual attacks on the system, there is no protection against accidental loss of votes. Electronic systems do fail. In South Brunswick, N.J. a machine failed and assigned votes in an arbitrary manner[xiii]. In such cases, there is no way to recover the lost vote from a completely electronic system.

A voting system should be designed to serve for many elections and many jurisdictions. The designer of the vote-casting mechanism will provide a template on which the election officials, for each election, assign candidates names to line numbers. This complexity makes accidental programming flaws more likely and gives greater freedom for malicious action by the designer, but it is also a significant security measure. No candidate's name appears in the voting software. The assignment of candidates to ballot places will vary with voting district. Open source software will prevent such tricks as: the designer embeds a hidden subprogram, which ensures that if ever a Hillary Clinton appears on the ballot, one out of every thousand votes cast for her will be randomly diverted to other candidates. The vote tabulation machinery should have the same independence. It knows only how many votes candidate number 7 received. A separate process collates candidate 7 with the candidate's name.

The dangers of direct record entry are well-recognized in the computer science community. Peter G. Neumann and Rebecca Mercuri sum up the issue in a January 2001 editorial in Communications of the Association for Computing Machinery, "Flawed though they may be, the paper-based and lever methods at least provide a visible auditing mechanism that is absent in fully automated systems."[xivxv]

Section 3: A proposal. We propose a method to record votes which meets the objections to both the card technologies and the direct record entry system. There are two aspects to our proposal: the interface and the vote record.

Interface: The voter enters his or her vote (which can be modified) either by touch screen or by pressing certain keys in the manner of an Automatic Teller Machine. The use of a screen allows design flexibility to make ballots more legible with larger type. The machine will not accept a vote that contains either two votes for the same office or fails to mark one choice (the choices include both abstain and write-in). These lockout provisions prevent both the under and over vote problems which plague both punch card and, to a significantly lesser degree, optical scanning systems.

Vote recording: Each voting station contains a printer. When the voter is satisfied with the ballot displayed on the screen, he presses `provisional vote' and a ballot showing the voter's choices for each office is printed. If the voter accepts this printed ballot, the voter presses `final vote', the machine records the electronic ballot and the voter deposits the printed ballot in the ballot box. If the voter finds an error in the printed ballot, he asks for a new ballot, the first printed ballot is marked spoiled, and the judge must reset the machine. Although an electronic record is maintained and used for the initial tally, the printed ballot is the official record available for a recount and for sampling to check the correctness of the DRE tally. To speed recounts, this ballot can be read by both humans (candidates' names) and scanners.

The advantages of this system include: the voter can quickly examine the printed ballot to see if his vote has been correctly recorded and computer interface rather than a marker provides more reliable recording of votes and permits `lockout'.

Section 4: Cost. Here are some rough cost estimates. There are several companies selling electronic voting systems. The current cost is around $3,000 per voting station [xvi] which serves around 100 voters (perhaps this number could be increased). There is a saving in printing costs estimated at $600,000 per election for Riverside County

[xvii](approximately 400,000 votes in the 2000 Presidential race). Thus, for the 4,600,000 voters in Illinois, a switch to entirely electronic voting would cost approximately 150 million dollars. While this is a large sum, the estimated savings in printing costs of 5% per year (more than the interest on borrowing the funds) makes it a feasible option. Our plan, which requires a printing device at each station, should increase the capital cost by less than 10% over a purely electronic system. Since only the ballots actually used are printed, the operating cost of the system might be lower than either punch cards or optical scanners.

Section 5: Conclusion. We propose criteria for secure elections and specific substandards for electronic voting. Our protocol contains two key innovations: voting on a computer screen with an `abstain option so that both undervotes and overvotes are locked out; printing at the polling place a machine and human readable ballot representing the voter's choice which is the official ballot. We further urge that to meet equal protection concerns states set minimal standards for ballot rejection of less than 1/2%. We stress that the optimistic remarks about security in this paper depend on our basic premise: we are describing a system in which voters come to the polls and vote on free standing machines. Phone voting, internet voting, and massively interconnected systems provide substantial and currently unacceptable security risks.

Acknowledgements: The idea that the voter approve a clearly inscribed ballot representing his choice was suggested to us by Taneli Huuskonen of the University of Helsinki; Bob Reynolds of UIC suggested that this record also be machine countable. While preparing this article we found such ideas mentioned in columns of Henry Norr[xviiixix]. See[xx] for a concise description of punch card, optical scanning and DRE.

John Baldwin, Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago.
Sharon Baldwin, Assistant Corporation Counsel, City of Chicago (This paper does not necessarily represent the views of the city.)
Marco Mazzucco, Laboratory for Advanced Computing, University of Illinois at Chicago

REFERENCES:

Neu93] Peter G. Neumann, Security Criteria for Electronic Voting: http://www.csl.sri.com/neumann/ncs93.html
[Sal93] R.G. Saltman. Assuring Accuracy, Integrity and Security in National Elections: The Role of the U.S. Congress. Position paper from *Computers, Freedom and Privacy '93,* pp. 3.8--3.17, March 1993.
[Sha93] M. Shamos. Electronic Voting --- Evaluating the Threat. Position paper from *Computers, Freedom and Privacy '93,* pp. 3.18--3.25, March 1993.

[1] Chicago Tribune, January 28, 2001

[i] 531 U.S 2000, Rehnquist, C.J. concurring, p. 9

[ii] Florida Supreme Court Nos. SC00-2346, SC00-2348 & SC00-2349. Page 15/

[iii] Report of the National Workshop on Internet Voting (Sponsored by NSF) www.internetpolicy.org

[iv] Chicago Tribune, March 1, 2001

[v] http://www.cpsr.org/conferences/cfp93/shamos.html.

[vi] 531 U.S 2000, per curiam, p. 4

[vii] Washington Post, 12/27/00 page 1

[viii] Chicago Tribune 12/24/00 page 1; Washington Post, 12/27/00 page 1

[ix] Eric Zorn column Chicago Tribune 11/18/00; based on Alter report of 1989.

[x] CNN 11-30-00, http://www.cnn.com/2000/ALLPOLITICS/stories/11/30/jackson.undervote/index.html

[xi] http://www.orlandosentinel.com/news/local/lake/orl-recount-12192000-story.story?coll=orl%2Dhome%2Dheadlines; see also Kausfiles, Slate 12/20/00: http://slate.msn.com/code/kausfiles/kausfiles.asp?Show=12/28/2000&idMessage

[xii] http://www.cpsr.org/conferences/cfp93/shamos.html.

[xiii] Home News Tribune 11/30/00: http://www.notablesoftware.com/Press/Malwitz.html

[xiv] Inside Risks 127, *CACM 44,* 1, January 2001; http://www.csl.sri.com/neumann/insiderisks.html

[xv] The web page of Rebecca Mercuri: **http://www.notablesoftware.com/evote.html** is a valuable resource.

[xvi] Legal analysis for San Francisco Board of Supervisors: http://www.ci.sf.ca.us/bdsupvrs/leganalyst/technology.htm

[xvii] The Desert Sun, 11/9/00: http://www.thedesertsun.com/news/stories/local/973729938.shtml

[xviii] Time to Digitize Elections, Henry Norr, San Francisco Chronicle, 11/27/00: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/11/27/BU91491.DTL

[xix] The Risks of Touch Screen Balloting, Henry Norr, San Francisco Chronicle, 12/4/00: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/12/04/BU91811.DTL

[xx] http://www.aceproject.org/main/english/em/emf02/default.htm