

**Testimony of *Donald F. Norris***  
**before the U. S. House of Representatives**  
**Committee on House Administration, Subcommittee on Elections**  
**Friday, March 23, 2007**

Madam Chairperson and members of the Committee,

Good morning. I am Don Norris, Professor of Public Policy and Director of the Maryland Institute for Policy Analysis and Research and of the National Center for the Study of Elections at the University of Maryland, Baltimore County. Thank you for the opportunity to present testimony about H. R. 811. In the time available this morning, I will address what I believe are serious limitations of the bill, particularly its requirement for a paper trail. I have provided the committee staff with my written testimony and have included a *Baltimore Sun* op-ed piece that I co-authored concerning Maryland's touch screen voting system.

First, let me say that the intent of the bill to require voter verification of ballots cast is a noble and worthy one. As a voter, I would want to be certain that my ballot is recorded as I cast it and tallied as recorded. The question is how best to accomplish this goal.

Unfortunately, the method set forth in the bill to achieve this goal is quite flawed. Its effect will be to require all of the United States to return to using paper ballots in elections; it will put an end to electronic voting, that is voting on Direct Recording Electronic voting systems (DREs); and it will significantly stifle or kill innovation in voting technology. As such, this aspect of the bill (requiring a paper trail) is a very bad idea. Here are several reasons why.

Paper ballots are notoriously susceptible to fraud. One of the main reasons that the nation moved from paper ballots to mechanical voting machines in the last century was because of the rampant fraud associated with paper ballots. Paper ballots can be (and frequently were) lost, stolen or damaged, and entire ballot boxes were lost, stolen or stuffed with counterfeit ballots.

Another problem with paper ballots can occur if they are required to be the official ballot of record. For example, if the printer on the VVPAT jams or if the optical scanner is misaligned, the paper ballot rules even though it may not be usable. This would effectively disenfranchise affected voters. Furthermore, this would be true despite the electronic machine correctly recording the voter's intention. The same would be true (disenfranchisement) if optical scan ballots were lost or stolen.

As a political scientist, I am far more concerned about the probability of election fraud with a paper ballot system than with an electronic system. This is because it takes far less skill to steal or otherwise compromise paper ballots than is required to compromise an electronic voting system. Ordinary people can tamper with paper. It takes considerable specialized knowledge about and skills with computer hardware and software to enable one to tamper with electronic voting systems. And it cannot be done casually. I'll come back to this presently.

One reason that proponents give for wanting to return to paper ballots is that “the people” are demanding the ability to verify on paper the votes that they cast on electronic voting machines. There is a minority of vocal, sometimes even strident individuals and groups that believe that this is the case. But the evidence does not support their claim. When asked, the great majority of voters do not share this view.

For example, three surveys conducted in 2006 (by me for UMBC, the *Washington Post* and the *Baltimore Sun*) showed that Maryland voters had high levels of confidence in the state's electronic voting system. As I said in testimony to the Maryland General Assembly about a year ago, there is no crisis of voter confidence in the Maryland touch screen voting system. And, as Doug Lewis noted in testimony earlier this week (March 20, 2007, p. 5), exit polls conducted for CNN in the 2006 election found that 88 percent of voters said that they had “full confidence” that their votes were counted accurately.

There is evidence, however, that voters do not want to and will not verify their votes even when given the opportunity to do so. In the Las Vegas precincts observed in

the 2004 Nevada election that used touch screen systems with voter verified paper audit trail or VVPAT units, less than 40 percent of voters actually did the verification. To put it differently, more than 60 percent of voters did not actually look at the VVPAT screen and compare what it displayed to results displayed on the DRE. Instead, they touched the DRE to indicate that they had verified, but without actually doing so. Evidently, they just wanted to vote and get out of the voting booth.

There are different ways to add paper to the election mix. One is the VVPAT. Another is the optical scan system. Both have limitations. Indeed, it is fair to say that there is *no perfect election system*, regardless of the technology employed and whether it uses paper or not.

Adding paper, whether VVPAT or an optical scan ballot will increase the time required to vote. And, in hotly contested elections with high turnout, this is not a trivial matter. Moreover, adding any further equipment to an election increases the complexity of election administration, increases the probability of equipment malfunction, and increases the need for election officials to be versed in how to connect, troubleshoot, repair or replace that additional equipment.

VVPAT technology involves printers and printers add complexity to election administration. They can also be expected to jam, creating problems for both voters and election officials. Printer jams can also violate the principle of the secret ballot.

Optical scan units that mark ballots (ballot marking systems) can fail due to calibration problems. They have to be maintained, transported, configured and set up absolutely properly or they can be subject to misalignment, thereby causing the ballot reader to be unable to count the voter's vote correctly. In one recent incident in Ohio, up to 20 percent of optical scan units had calibration problems that resulted from being juggled or worse during transport ("Problems found in voting machines" at [newarkadvocate.com](http://newarkadvocate.com), accessed March 21, 2007).

Optical scan systems that require voters to manually mark their ballots are subject to all of the problems we have seen in the past where voters do not mark their ballots properly. The ballots, therefore, cannot be counted or are counted incorrectly and leave the voter's intent unclear.

Another reason that proponents give for paper ballots is the need to audit elections and conduct recounts. In nearly every election where recounts are undertaken of paper ballots, the vote tallies completed manually by human beings produce inconsistent and sometimes conflicting results. Think of Florida in 2000 and the State of Washington in 2004. Ironically, by the way, the contesting parties in Washington did not request recounts in precincts where electronic voting was used. Furthermore, and contrary to claims made by at least some paper trail advocates, electronic systems can be audited and will produce a record of all ballots cast on them.

The claim that electronic voting systems are insecure is based on a dubious assumption that goes something like this. Given the right tools, the right amount of time, and unfettered access to an electronic voting machine, a knowledgeable person can insert malicious software to produce erroneous results. This is a hypothetical if not far-fetched scenario. And it has not happened in an election to date. Further, as Finnish computer programmer Harri Hurtsi demonstrated, optical scan systems are as subject to hacking as DREs.

The security around the touch screen system in Maryland, for example, is designed to prevent such an occurrence, and it can be improved to discover and rectify fraud should an attempt be made. I suspect that the same can be said for electronic voting systems in other states. Security around electronic voting systems may not be perfect, but it is far tighter than security has been historically true of paper ballots.

It is said that electronic voting systems are inherently subject to tampering and fraud. I've already shown how insecure paper systems are and I think it fair to say that electronic systems are more secure than paper, so I won't go there again. But the fact is

that there is no evidence to show that electronic systems have actually been tampered with or otherwise compromised in any elections in the U. S. In Maryland, for example, the state's the touch screen system has performed well in the 2004 and 2006 primary and general elections. Votes on touch screen machines were accurately recorded and reported and no one has challenged the results based on the performance of these machines. And, as I said earlier, voters responding to scientific surveys said that they had high levels of confidence in the state's touch screen voting system (which, by the way, does not have paper).

It is also true that security can be increased around electronic voting systems to further ensure that they cannot be compromised. Just because electronic voting systems are computers does not mean that they will necessarily be subject to fraud and attack. For example, my colleague Prof. Paul Herrnson at the University of Maryland, College Park, and I have suggested that Maryland's system of parallel testing be expanded to provide even higher levels of confidence that the state's touch screen systems have not been compromised. Expanding parallel testing would be a far less costly and highly effective method of preventing and/or detecting attacks on this system than completely replacing the system, especially one that has worked well in successive elections.

I would echo what computer scientist Michael Shamos of Carnegie Mellon University said in testimony before this committee last fall (September 28, 2006). Most of the technical problems associated with DREs have been fairly minor and, more importantly, all have been or can be rectified. Therefore, there is no compelling technical reason to abandon electronic voting technology. To do so would be akin to "throwing the baby out with the bath water."

Finally, as written H.R. 811 will stifle if not kill innovation in voting technology for many years. Some promising, independent vote verification technologies are being developed today, although as a study that my colleagues at UMBC and I conducted last year found none is yet market ready.

([http://www.umbc.edu/mipar/documents/VoteVerificationStudyReport-FINAL\\_001.pdf](http://www.umbc.edu/mipar/documents/VoteVerificationStudyReport-FINAL_001.pdf))

If this bill is adopted as written, any incentive for scientists and entrepreneurs to continue to innovate around the issue of vote verification will be eliminated because nothing but a paper verification system would be allowable under the law. This would be particularly unfortunate because it would deny us the opportunity benefit from innovation in this important area. Also, as my UMBC colleague Prof. Alan Sherman has noted, the goal of verification should be to allow the voter to know that his or her ballot was cast as intended, recorded as cast, and tallied as recorded. Paper verification systems cannot do the last step, but some of the emerging technologies can.

For all of these reasons, it is my strong recommendation that you consider amending H. R. 811 to require independent vote verification, but to remove all references to any particular technology for doing so. Let state and local governments figure out how best to do this, and let the marketplace develop new and better solutions.

**-End-**

**Donald F. Norris** is Professor of Public Policy and Director of the Maryland Institute for Policy Analysis and Research (MIPAR) and of the National Center for the Study of Elections (NCSE) at the University of Maryland, Baltimore County (UMBC). He is a specialist in urban politics, public management, and the adoption, management and impacts of information technology (including e-electronic government) in public organizations. Dr. Norris has published five books with two under preparation. He has published more than 50 articles in scholarly journals and chapters in scholarly books and nearly 100 monographs, reports and scholarly papers. Dr. Norris operates a website in partnership with the Maryland State Board of Elections that provides information to voters about candidates for election, campaign finances and voter registration status (<http://mdelections.umbc.edu>). Dr. Norris was founding editor-in-chief of the *International Journal of Electronic Government Research*. He holds a B.S. in history from the University of Memphis and an M. A. and a Ph. D. in government from the University of Virginia. He can be reached at [norris@umbc.edu](mailto:norris@umbc.edu) or 410 455 1080. His websites are: [www.umbc.edu/mipar](http://www.umbc.edu/mipar) and <http://www.umbc.edu/mipar/ncse>.

**A slightly modified version of the following was printed as an op-ed in the *Baltimore Sun* on February 26, 2007.**

Momentum is developing within the Maryland General Assembly to get rid of the state's perfectly functional touch screen voting system and replace it with an optical scan voting system that uses paper ballots. This proposed change is not only unnecessary, it would have negative consequences that no one, including proponents of paper ballot/optical scan voting systems, will like.

It is fair to say that the touch screen system has performed well. Votes on touch screen machines were recorded and reported accurately in the 2004 and 2006 primary and general elections. No results have been challenged based on the performance of these machines. Problems in recent elections involved human error and electronic poll books, not the touch screen voting system, and the problems were corrected.

Proponents of "opscan" voting systems give two principal reasons for replacing touch screen machines. First is the assertion that computer-based systems are inherently susceptible to fraud and attack. Given the right tools, time, and access to an electronic voting machine, they posit, a knowledgeable person can insert malicious software to produce erroneous results.

It is important to note that this is a hypothetical scenario. The security around the touch screen system in Maryland is designed to prevent such an occurrence, and it can be improved to discover and rectify fraud should an attempt be made.

Second is the dubious claim that voters lack confidence in the touch screen system. Public opinion surveys indicate that Maryland voters like the touch screen system. Surveys conducted last year by the University of Maryland, Baltimore County, The Washington Post, and the Baltimore Sun all found that voters had high levels of confidence in the touch screen system. Moreover, a study conducted at the University of Maryland, College Park that compared the Maryland system to other voting systems found that, in terms of voter trust, overall satisfaction, the need for help, and ability to vote as intended, the Maryland system performed better than most of the others.

Why fix the system if it is not broken? And why fix it if the alternative will present its own range of problems?

Paper is not tamper-proof. Finnish computer programmer Harri Hurtsi was able to hack into an optical scan system that uses paper ballots. Paper is also notoriously insecure. Opscan systems requires local election judges to manage millions of paper ballots on election day, transport them to the local election boards after the election is over, and store them securely. This nation's long and inglorious history of ballot theft suggests that there is plenty of opportunity for mischief.

Opscan voting systems do not prevent errors. Voters are more likely to select the wrong candidate or commit undervotes or overvotes when voting on paper than when using the state's touch screen system. The evidence further shows that voters who try to change their votes or cast write-in votes also make more errors when using paper. This may be because, unlike touch screen systems, opscan systems have no review screen. And in the event of a controversy, recount discrepancies can occur with paper ballots, as we well know from Florida in 2000 and Washington State in 2004.

At a time when the state faces a budget deficit, we question the wisdom of the General Assembly spending upward of \$40 million to replace a voting system that has worked

well, that voters like, and in which they have high levels of confidence. Those who are concerned about voting security should instead turn their attention to ensuring that the State Board of Elections significantly expands its current program of parallel testing, whereby election officials cast votes and then check the accuracy of the votes recorded on a sufficient number of randomly selected voting systems to ensure that no foul play has been committed.

There will be costs associated with expanding parallel testing, but they will be a small fraction of the cost of a replacement system.

---

Donald F. Norris, Ph. D.  
Professor of Public Policy  
Director, Maryland Institute for Policy Analysis and Research and  
National Center for the Study of Elections  
University of Maryland, Baltimore County

Paul S. Herrnson, Ph. D.  
Professor of Political Science  
Director, Center for American Politics and Citizenship  
University of Maryland, College Park

In 2005-6, Dr. Norris led a UMBC team that examined vote verification technologies for the Maryland State Board of Elections. In January of 2006, He also conducted a survey of the opinions of Maryland voters about voting technology. Both are available at ([www.umbc.edu/mipar/research.html](http://www.umbc.edu/mipar/research.html)).

Beginning in 2001, Dr. Herrnson has led a team of researchers from UMCP, the University of Michigan, the University of Rochester, and Georgetown University in several studies of voting systems and vote verification systems that were funded by the National Science Foundation, the Carnegie Corporation of New York, and the Maryland State Board of Elections. He is co-author of Voting Technology: The Not-So-Simple Act of Casting a Ballot to be published by the Brookings Institution Press in 2007.