Teresa Hommel's voting machine simulation, "Fraudo, the Fraudulent Voting Machine," has been used internationally to help people understand the security problems with computers used in voting. "Fraudo" is featured on Ms. Hommel's web site, WheresThePaper.org. Ms. Hommel has worked with computers since 1967. This article is available at www.wheresthepaper.org/DREsViolate5thPrinciple090627.pdf

Unitarian Universalist Association of Congregations
48th Annual General Assembly, A Meeting of Congregations
Salt Lake City, Utah, Saturday, June 27, 2009
Workshop #4069 - Saturday 5:15-6:30pm, Salt Palace – 253

Does Touchscreen Voting Violate the 5th Principle?

Teresa Hommel, Chairwoman,
Task Force on Election Integrity, Community Church of New York

First I want to say that I will end on a positive note, even though I'm going to talk about the problems we face.

1. I have some starting assumptions about "representative democratic government" and the role of "we the people."

In a representative democracy, there is a need for government to do its work in public and another need for the people to show up and provide oversight, which means to understand government's work, give guidance for it, and keep a watchful eye on it.

Government behind closed doors is easily corrupted. It might be honest, but we don't know. So we need our government not only to be honest, but also to maintain the appearance of honesty. "The appearance of honesty" is another way of saying that government must do its business in public, and not hide behind closed doors.

2. With these starting points, what's wrong with electronic voting and vote-counting?

First, we have two kinds of electronic equipment in American elections.

2.a. Touchscreen-style voting machines (pushbutton versions are also in use).[1]

In 2008, 33% of Americans voted on electronic voting machines,[2] usually called touchscreens. The voter touches the screen of the computer to indicate their votes, and the computer handles everything after that including printing a tally report at the end of the election day.

---

[1] These machines, whether they let voters indicate their votes by touching a touchscreen or pushing a pushbutton, are known as "DREs" which stands for "Direct Recording Electronic" voting machines. They mimic the function of the old mechanical lever voting machines which are "direct recording mechanical." However, the lever machines are single-purpose mechanical devices; in over 100 years of use, a culture of fraud never developed around them because they are too cumbersome to tamper with and a person with brief training can look in the back at the large, easy-to-see rods and gears and see any problems. In contrast, DREs are inviting to fraud that can be accomplished without leaving any evidence, and the communications capability in most DREs makes tampering even easier.

[2] http://www.electiondataservices.com/images/File/NR_VoteEquip_Nov-2008wAppendix2.pdf

With touchscreens, voters can't witness their own votes being recorded and cast. They can see what's visible on the screen, but they can't know if that's the same as what's recorded internally in the electronic memory. It might be the same, but it might be different.

And election observers can't witness the storage, handling, and counting of votes. No one knows whether the computer is doing these things correctly, or if the tallies are accurate. That "no one" includes observers, voters, election administrators, and candidates.[3]

Some touchscreens have a paper trail and some don't, but the paper trail idea--to which I devoted several years of my life--is now recognized as a failed idea.[4] So please don't leave here thinking "we need a paper trail." We used to think that, but it didn't work out because:

a. Most voters can't verify accurately. We have a CalTech/MIT study showing that test voters found NONE of the errors in 108 test elections with paper trails containing errors.[5] And the Rice University study showing that two thirds of test voters didn't notice when 8 races disappeared from their review screen.[6]

b. Election administrators don't have the resources to perform audits to verify correct computer function. Even if they had the resources, they don't want to do that kind of work.[7] They don't think they should have to. They think it is an unfair burden to ask them to conduct audits, and they want to treat the computers the way they used to treat the old mechanical lever machines. At one time those old babies were used by 74% of American voters, and New York still uses them. They don't need audits because they are mechanical single-purpose machines--you just open the back and look in and say, "Yup, it's fine." The rods and gears are large and easily visible.

c. Third, many of the printers that vendors have supplied to print the paper trail were, or are, so shoddy that they don't work. That probably means the vendors had to work really hard to find printers that could not print 200 slips of paper in a 12-hour day, because every cash register and gas pump in America does that with ease.

2.b. Voter-marked Paper ballots and Precinct-based Optical Scanners.

In 2008, 56% of Americans voted by marking a paper ballot--darkening in a little oval next to their candidate's names, or drawing a line next to the name--and then inserting their ballot into an electronic vote-counting machine, called an optical scanner or just plain "scanner."[2]

The scanner reads the marks to determine who the votes are for, like a Scantron used to grade tests for school kids, or the scanners used to read marks on lottery cards.

With paper ballots and scanners, voters create an authentic first-hand record of their intent on paper, which is excellent. But then the paper is handled and counted inside the scanner, so we

---

[3] For a sampling of 179 DRE failures that cause long lines and frustrated would-be-voters: http://www.votersunite.org/info/DREFailedExperiment.pdf

[4] http://www.wheresthepaper.org/VVPAT_Idea_Failed.pdf

[5] http://www.vote.caltech.edu/drupal/files/working_paper/vtp_wp31.pdf

[6] http://www.wheresthepaper.org/SarahPEverettDissertation.pdf , Everett, S. P. (2007). Doctoral dissertation, Rice University, Houston, TX. See especially, discussions on page 77 and 103.

[7] http://www.wheresthepaper.org/HouseAdminTestimonyDougLewis3_20_2007.pdf

can't know if the votes were read accurately, or credited to the intended candidate, or if the tallies are accurate. Here's a report summarizing 186 scanner failures,[8] and one common problem is for the ballot programming to have errors, and to credit votes to the wrong candidates.

Then, worse, at the close of polls, the whole ballot box full of paper ballots is taken away, out of observers' view, at which point the ballots lose their authenticity.

Some jurisdictions might do a hand-to-eye recount several days or weeks later to determine whether hand-count tallies confirm the scanner tallies. However, without continuous public observation of the ballots from the close of polls until the recounts, we can't know whether the ballots in the recount are the same ballots that were cast on election day. I'm not saying they are the same, or they're not. I'm saying we can't know.

Some people say they "trust the computer." Many people say they trust their election administrators. But trust and trustworthiness are not the issue here. Innocent versus malicious errors in ballot programming is not the issue.

The issue is, if we want to live in a democracy, we have to maintain the proper relationship between "we the people" and our government. Votes behind closed doors are easily corrupted, and we can't know if they have been corrupted or not.

2.c Chaos.

What we have with electronic voting (touchscreens or pushbuttons) and electronic vote-counting (paper ballots and scanners) is "chaos," a state of not knowing and not being able to know.

With this equipment "we the people" have lost oversight, and our election administrators have lost control, of our election processes. We really don't know if the winners of our elections were selected by the voters, innocent errors in programming, or malicious electronic tampering.

With the technology of paper ballots and scanners, you can add paper ballot tampering to the list of possibilities that we don't know about, unless observers are allowed to watch the voted ballots continuously from close of polls until the election is certified. In case you think this is an extreme position, I want to repeat to you what two elderly ladies once told me. They were the Democrat and Republican election commissioners of one of our New York counties. "We tell everyone what we are going to do. We tell'em when and where. And we tell'em, you better show up and watch, because we don't want you coming around later and telling us we did it wrong."

With electronic ballot images, produced by the newer scanners, you can add electronic image tampering to the list of possibilities--an attractive idea because the whole electronic ballot box fits on a memory card the size of a postage stamp, and you can do most of your tampering on your laptop at Starbucks or in the privacy of your own home in your pajamas.

---

[8] "Ballot-Scanner Voting System Failures in the News - A Partial List," May 22, 2009. Describes 186 occurrences of malfunction including 80 incorrect tallies, 35 EMS miscounts, 22 memory card failures, 5 mark-detection failures, 13 instances of misprinted ballots, and 31 miscellaneous operational failures. Readers are cautioned to remember that although scanners have many failures, they are superior to touchscreen-style voting machines (called DREs) which have more failings and 3 times more failures. http://www.votersunite.org/info/OpScansIntheNews.pdf

3. What if?

What if the computers were perfect? They would still be inappropriate because they undermine our democracy by preventing government from conducting its business in public and preventing the people from exercising oversight.

And then there's the reality--our electronic voting and vote-counting equipment is not perfect. We have thousands of documented failures of both touchscreens and scanners, with a ratio of about 3 to 1. We have dozens of computer science studies saying the equipment was not designed to be secure, not even designed according to the most basic professional standards.

Is there such a thing as a secure computer? The largest computer crime survey ever conducted--the FBI Computer Crime Survey of 2005[9]--reported that 87% of organizations were aware that they had had security incidents in one year, with 20% having 20 or more incidents. 64% of organizations lost money, showing that the incidents were serious, not trivial. 44% had incidents perpetrated by their own insiders. If these numbers hold true for election boards, it means approximately two in five can expect insider computer tampering.

The FBI's survey showed that even companies that know the most about security, much more than any election board, still can't protect their own money. It means that computers are inappropriate for use in elections because they introduce unmanageable risks and vulnerabilities, and we don't need computers in the first place.

What we need is people. Huge numbers of people--as voters, poll workers, observers, and vote-counters.

4. More negatives: privatization and an infrastructure for nationwide tampering.

4.a. Electronic voting and vote-counting have privatized our elections, leading to price gouging and spiraling costs for local election boards.[10]

But the problems run deeper.

4.b. We have replaced an infrastructure for local control of elections with an infrastructure for nationwide control. And this creates an infrastructure for nationwide tampering.

The history of fraud in American elections appears to be a history of cheating by a patchwork of local bosses. Regardless of different election technology over the years, cheating has always taken place when observers were not allowed to observe, and if irregularities occurred investigators were not allowed to investigate or gather evidence.[11]

Nowadays our electronic voting equipment itself prevents observation. If irregularities occur, our laws and courts have consistently prevented inspection of equipment and software due to its

---

[9] FBI 2005 Computer Crime Survey http://www.WheresThePaper.org/FBI_ComputerCrimeSurveyPR.pdf

[10] Electionline, Feb. 19, 2009 http://www.WheresThePaper.org/Electionline090220StateCtyElecOfficesEconomicCrisis.htm

[11] Deliver the Vote, 2005, by Tracy Campbell, Carroll and Graf Publishers. Also, Election Administration in the United States, 1934, by Joseph P. Harris, Ph.D., at http://vote.nist.gov/election_admin.htm

being proprietary and trade-secret. This is why we sometimes hear "there's no evidence that electronic voting equipment has ever been subject to fraud."

What's different today is:

First, nationwide, three companies provide most of our computerized election equipment and almost all of the equipment has wireless and other communications capability. This creates the infrastructure for consolidated cheating nationwide, replacing the local bosses of yesteryear.

Second, despite talk about outside hackers, corporations are now the new insiders--more "inside" with more access and control over votes and tallies than our local election administrators. This creates enormous opportunity for tampering.

Do I believe that cheating takes place through e-vote machines? Of course. The original e-voting machines were designed so there was no way to determine if they were working accurately or not. I've been a computer professional for 42 years, and that's a red flag to me. You don't design equipment like that unless you have certain intentions. And despite the perfection of printing technology in the last hundred years, the fact that paper trail printers don't work well enough to produce a useful paper trail—isn't that another red flag? And there are others.

4.c. Until recently our election administrators fully understood and fully controlled their technology and procedures, whether they used paper ballots, mechanical lever voting machines, public declaration of votes through a show of hands, etc.

Computers have removed our election administrators from control.[12] If vendors refused their support and services, many jurisdictions would not be able to hold elections. Election administrators can no longer comply with their legal (and in some states constitutional) mandate to oversee their elections because they are technically naïve. They don't have the interest, time or resources to become computer experts. Running elections is a big job already, and it is unrealistic to expect our election boards to take on a second big job--to run secure computers--when the FBI survey shows that our most knowledgeable corporations can't achieve that.

5. Historical Perspective, how did we get here?

Over the last 38 years we have seen nearly every area of our lives come under the influence, control or privatization by large corporations: food production, medical care, pharmaceuticals, environment, education, energy, news media, communications, conduct of war, manufacturing, off-shored jobs, our prison system, financial institutions, management of our economy, and our political parties. It is difficult to think of any area of our lives that have not been touched by corporate interests.

Each area came under corporate control in its own particular way, but we need to take a high-level overview if we want to see the commonality, if we are going to counteract it.

I think most of us realize that our government is now more responsive to corporate interests than to the will of the people. Each of us may have our pet area, such as healthcare or the war in Iraq,

[12] Ellen Theisen, VotersUnite.Org: "Vendors are Undermining the Structure of U.S. Elections" http://www.votersunite.org/info/ReclaimElections.pdf

but we need to understand how we got into our current mess if we are to unravel it and reassert government by the people.

I said 38 years, because in 1971 Lewis Powell, who later served fifteen years on the U.S. Supreme Court, wrote a memorandum for the U.S. Chamber of Commerce to lay out his ideas for how business could become more influential in American government and culture.[13] The Powell memo laid out the original plan for what we are dealing with today. He called for pro-business:

a. faculty in university departments of political science, economics, sociology, and history.

b. evaluation and re-writing of textbooks.

c. speakers at colleges, law schools, and business schools.

d. influence on high schools.

e. content in our news media, including television, radio, press, scholarly journals, popular magazines, books, paperbacks, pamphlets, paid advertisements.

f. lobbyists to influence staffers and elected officials at the national, state, and local level.

g. influence in our courts, which he called "a vast area of opportunity"

h. corporate expenditures to create national organizations.

Powell suggested that these efforts should last for "an indefinite period of years," by which he meant decades. His memo was followed by an unprecedented wave of political organizing by business executives who created foundations, think tanks, litigation centers, publications, public relations offices, lobbying agencies, short-lived coalitions to fight for or against specific issues, phony grassroots movements, Political Action Committees, and "soft money" for political parties.

If I had more time, I would lay out how electronic voting arose from the corporate efforts that implemented Powell's memo.

The most dangerous threat we face is the result of a subtle and very successful public relations effort that has shifted our ideas about what makes good elections.

- We have gone from "get it right on election night" to "if the tallies are potentially verifiable we don't need any actual verification."

- We have gone from knowing that observers are the only way to get honest elections, to believing that it is more important to use computers because they are modern.

- We have gone from knowing that citizens have to show up in person and exercise meaningful oversight of government to maintain a democracy, to thinking that staying home and watching election returns on TV is good enough if you "trust" your election administrators.

[13] http://www.wheresthepaper.org/keydocs.html, number 37 has the links.

Another very dangerous reality is that while corporations have spent huge amounts of money to amplify their voice, they have also spent money to silence the voice of our good government groups on at least one issue—my issue, the issue of citizen oversight of election procedures with votes after the votes have been cast.

Our national good-government groups all want to "get out the vote." Not one of them will touch the question of what happens to the votes once cast, the fact that citizen oversight of an e-vote computer is meaningless, and the fact that most of our election administrators are so unknowledgeable about their technology that they wouldn't know if their tallies were being tampered with right in front of them.

I believe that corporate money is behind this inappropriate and universal silence of our good government groups[14], and also behind advocacy of election "conveniences" like Instant Runoff Voting which require computerization.

6. What it will take to revitalize our democracy?

a. Our schools need to start teaching civics starting in kindergarten (age-appropriate).

b. We need to educate ourselves and our youth. We need to prepare our best and brightest, most honest and idealistic youth for careers in public service.

c. We have to pay attention to our governmental infrastructure. We have relatively many UU issue experts, but we don't have many people who are dealing with privatization of the infrastructure of our culture and government. We don't have a Lewis Powell in reverse.

d. We need to move beyond thought and study to long-term, sustained involvement and action, both individually and in groups. For most of us that means learning new skills, doing things for the first time which can feel really uncomfortable, and showing up and speaking in the offices, halls and hearing rooms of our government.

e. We need to join our political parties and work our way up, and become the voice and decision-makers of our parties.

f. We need to develop a continuing relationship with our media, writing letters to the editor and articles, as well as complaints when the news is partial, biased or not reported at all.

7. The delicate problem of voter confidence.

There is a realistic concern that telling people electronic voting and vote-counting are a scam will suppress the vote. But there is a worse realistic concern--if we don't educate people and make changes, we are supporting a mass lie and our elections may be reduced to nothing more than a public ritual.

The ritual of elections, in and of itself, does not make a democracy. We know this from various dictators:

[14] For example, the ACLU. http://www.wheresthepaper.org/news.html#ACLU

Josef Stalin: "It's not who votes that counts, it's who counts the votes!"
Anastasio Samoza of Nicaragua: "You won the vote, but I won the count."
Boss Tweed of New York: "As long as I count the votes, what are you going to do about it?"

8. Conclusion

I became a full-time election integrity activist in 2003. In 2004 I published an article in UUWorld called "Don't turn democracy over to computers."[15] We have some copies here, if anyone would like to read it now. What astonishes me, reading it after five years, is that almost all of it is still relevant—except for the advocacy for paper trails.

I said I would end on a positive note. I will quote Margaret Mead.

"Never doubt that a small group of thoughtful, committed citizens can change the world. Indeed, it is the only thing that ever has."

I have come to believe that this is true from my own small, individual experience.

I am entirely hopeful that we Unitarian Universalists can rise to the challenge to help our nation revitalize our democracy. All we need is a clear understanding of what we face and a lot of hard work, with our Fifth Principle[16] supporting us, and our congregations working with us.

# # #

[15] http://www.uuworld.org/2004/06/forum.html

[16] http://www.uua.org/visitors/6798.shtml 11/7/08:

There are seven principles which Unitarian Universalist congregations affirm and promote:

1. The inherent worth and dignity of every person;
2. Justice, equity and compassion in human relations;
3. Acceptance of one another and encouragement to spiritual growth in our congregations;
4. A free and responsible search for truth and meaning;
5. The right of conscience and the use of the democratic process within our congregations and in society at large;
6. The goal of world community with peace, liberty, and justice for all;
7. Respect for the interdependent web of all existence of which we are a part.

Unitarian Universalism (UU) draws from many sources:

1. Direct experience of that transcending mystery and wonder, affirmed in all cultures, which moves us to a renewal of the spirit and an openness to the forces which create and uphold life;
2. Words and deeds of prophetic women and men which challenge us to confront powers and structures of evil with justice, compassion, and the transforming power of love;
3. Wisdom from the world's religions which inspires us in our ethical and spiritual life;
4. Jewish and Christian teachings which call us to respond to God's love by loving our neighbors as ourselves;
5. Humanist teachings which counsel us to heed the guidance of reason and the results of science, and warn us against idolatries of the mind and spirit.
6. Spiritual teachings of earth-centered traditions which celebrate the sacred circle of life and instruct us to live in harmony with the rhythms of nature.

These principles and sources of faith are the backbone of our religious community.