AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ELECTION REFORM: MACHINES AND SOFTWARE

HEARING

BEFORE THE

SUBCOMMITTEE ON ELECTIONS

COMMITTEE ON HOUSE ADMINISTRATION

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MEETING HELD IN WASHINGTON, DC, MARCH 15, 2007

Printed for the use of the Committee on House Administration

Available on the Internet:
http://www.gpoaccess.gov/congress/house/administration/index.html

U.S. GOVERNMENT PRINTING OFFICE

35–805 WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOUSE ADMINISTRATION

JUANITA MILLENDER-McDONALD, California, *Chairwoman*

ROBERT A. BRADY, Pennsylvania
ZOE LOFGREN, California
MICHAEL E. CAPUANO, Massachusetts
CHARLES A. GONZALEZ, Texas
SUSAN DAVIS, California

VERNON J. EHLERS, Michigan
Ranking Minority Member
DANIEL E. LUNGREN, California
KEVIN McCARTHY, California

SUBCOMMITTEE ON ELECTIONS

ZOE LOFGREN, California, *Chairwoman*

JUANITA MILLENDER-McDONALD, California
CHARLES A. GONZALEZ, Texas
SUSAN DAVIS, California

KEVIN McCARTHY, California
VERNON J. EHLERS, Michigan

ELECTION REFORM: MACHINES AND SOFTWARE

Thursday, March 15, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ELECTIONS,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, D.C.

The subcommittee met, pursuant to call, at 2:25 p.m., in room 1539, Longworth House Office Building, Hon. Zoe Lofgren (chairwoman of the subcommittee) presiding.

Present: Representatives Lofgren, Millender-McDonald, Davis of California and McCarthy.

Staff Present: Tom Hicks, Counsel; Janelle Hu, Professional Staff Member; Matt Pinkus, Professional Staff/Parliamentarian; Kristin McCowan, Chief Legislative Clerk; Gineen Beach, Minority Counsel; Peter Sloan, Minority Professional Staff; Salley Collins, Minority Press Secretary; and Fred Hay, Minority General Counsel.

Ms. LOFGREN. Welcome to the first Subcommittee on Elections and Election Reform. I am honored to be serving as Chair of this subcommittee, and I look forward to working with our Ranking Member Mr. McCarthy, my colleague from California, as well as the rest of the committee as we look at our election systems and make sure that we have the best that we possibly can in our country.

The purpose of this hearing is to begin to look at election reform, specifically the tools of voting machines, software, and making these tools accessible to all. In accordance with the rules of this committee, witnesses will have 5 minutes for their testimony and may submit written testimony, and any Members wishing to submit opening remarks for the record may do so, although, of course, the Ranking Member is welcome to make an opening statement.

[The statement of Ms. Lofgren follows:]

Committee on House Administration
Subcommittee on Elections

Election Reform Hearing
"Machines & Software"
Thursday, March 15, 2007

Opening Remarks

Welcome to the first Subcommittee on Elections of the Committee on House Administration hearing. I am honored to be serving as Chair of this subcommittee and look forward to working with Ranking Minority Member of the Subcommittee Mr. McCarthy and the rest of the committee. The purpose of this hearing is to begin to look at election reform, specifically, the tools of voting: machines and software and making these tools accessible to all.

The Help America Vote Act (HAVA) provided funds for state and local government units to replace outdated punch card systems with more advanced machines. In order to have received the funds, states and local government units were required to develop a plan to upgrade their voting systems. Unfortunately, the nation still has not fixed the machinery of voting.

All systems need better testing, maintenance and independent certification. All systems must be auditable. Besides being auditable, these systems and the software used in them must be open. The idea behind open source is very simple: When programmers can read, redistribute, and modify the source code for a piece of software, the software evolves. It can be improved and adapted.

Numerous reports from the GAO, our colleagues in the Judiciary Committee, the Secretary of State of California, and academics have called for greater accountability in voting machines and software. Voting system software should be publicly disclosed. All systems must also allow voters with disabilities to vote privately and independently.

We need to better define voting system standards. I am excited to have these two panels before us to discuss pertinent issues in election reform. Changes are needed. This hearing and any future hearing are an opportunity for us to hear what possibilities are out there to make significant improvements in our election system.

Ms. LOFGREN. Our apologies to everyone here. The House has had an open vote for a considerable period of time while the President was here, and it has really gotten our schedule out of whack. So if it is possible for witnesses to make their summary even less long, 3 minutes, that would be a good idea, because we do have another panel, and I can assure you we will read your entire written testimony. That would be very helpful in making sure that everyone gets heard.

We are debating to replace outdated punch-card systems with more advanced machines. Unfortunately, the Nation still has not fixed the machinery of voting. All systems need better testing, maintenance, and independent certification. All certifications need to be audited, and besides being audited, these systems and software used in them must be open.

When programs can redistribute and modify the source code, the piece of software that is involved can be improved and adapted. Numerous reports are calling on the Judiciary Committee for this. The secretary of state of California, and academics call for greater accountability on voting machines and software, and we know that as we do this, we need to make sure that our fellow Americans who have disabilities are accommodated fully as they also join us in voting at the polls. We cannot ignore those with disabilities, and clearly we have no intention of doing so.

I am excited to have these two panels before us, and now I would like to recognize my colleague from California, the Ranking Member Mr. McCarthy.

Mr. MCCARTHY. Well, I want to thank the Chair for having this hearing. I think this is something we should do always; not wait until we believe there is a problem out there with elections, but we should always analyze them, look at what we are using, and continue to have America having one of the most honest elections throughout this world.

But in light of time, I will submit my remarks and leave more time to listen to you so we can have some questions.

Thank you.

[The statement of Mr. McCarthy follows:]

Congressman McCarthy's Opening Statement
Committee on House Administration
March 15, 2007

I thank the distinguished Chairwoman and fellow Californian, Congresswoman Zoe Lofgren, for holding this hearing that looks into a fundamental aspect of our democratic process.

Today, the Subcommittee on Elections convenes for the first time since it was formed earlier this year. At this hearing, we will examine an issue at the heart of our democracy and American liberty, free and fair Federal elections. I'm sure my Democratic and Republican colleagues will join me in agreeing that if this Subcommittee is going live up to its mission of ensuring free and fair House elections, we need to operate with fairness, honesty, and partnership.

Before I was elected to Congress, this Committee wrote the Help America Vote Act. Two of the primary purposes of the Help America Vote Act were to increase security requirements for voting systems and to expand access to individuals with disabilities so that they are able to vote. Reforms in the Help America Vote Act assisted many Americans when voting in last years' election and all 435 results were certified by their respective states for being free and fair elections. But this committee should still be proactive. After every election, we should examine our current voting system and fully examine the big picture and ask:

With cost and technological advances considered, can we make improvements to our voting system to make it the best for American voters, relative to other voting options and alternatives? By accepting a new voting system, will we run into problems that we had before the Help America Vote Act? Will changes to our current voting system prevent or make it more difficult for disabled Americans from voting? These are all broad questions and considerations that this

Subcommittee must consider if we are to ensure Americans are given the most honest and fair process of electing their federal voices.

At this hearing, we need to look at ways to define our measuring stick of success for elections. If there are proposals to improve our voting system, no matter how contentious, it is incumbent on this Subcommittee to figure out why that election reform would be an improvement from the current system and what tradeoffs will be made. In that broader discussion, we must ask the tough questions, debate all the issues, and push the best and most feasible idea at the end of the day.

I thank the witnesses for joining us today to examine these critical issues and I look forward to hearing their testimony and answers to our questions.

Ms. LOFGREN. And we have been joined by another Californian, my colleague Susan Davis.

Ms. LOFGREN. So we will begin with our witnesses, and if we can start with Mr. Pierce and move right along the panel. Welcome.

STATEMENTS OF KELLY PIERCE, DISABILITY SPECIALIST, COOK COUNTY, ILLINOIS, STATE'S ATTORNEY OFFICE; ERIC CLARK, SECRETARY OF STATE, STATE OF MISSISSIPPI; DIANE CORDRY GOLDEN, Ph.D., DIRECTOR, MISSOURI ASSISTIVE TECHNOLOGY; AND TED SELKER, Ph.D., DIRECTOR, VOTING TECHNOLOGY PROJECT, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

STATEMENT OF KELLY PIERCE

Mr. PIERCE. Thank you, and if you could, Madam Chairwoman, warn me about a minute before my time is up.

I am coming here as a disability specialist at the Cook County State's Attorney's Office and a member of the accessibility committees of the Cook County Clerk's Office and the Chicago Board of Election Commissioners.

I have worked extensively on disability-related technology issues since the early 1990s. I have worked specifically on systems regarding audio systems, regarding automatic teller machines for large financial systems, including J.P. Morgan-Chase, LaSalle Bank, and American Express, and most recently on developing the voting system that Chicago and Cook County implemented starting last year.

I became blind in 1985, and for the past two decades, I have used someone to vote for me except for last year. During those two decades, I endured different kinds of experiences, often humiliating and degrading, poll workers who seemed illiterate, who could barely read the ballot or had to spell candidates' names to me. Some poll workers had difficulty even seeing the ballot. Other times it was friends who would reveal my votes to other people that I turned out to be somewhat embarrassed about or humiliated about. And once I had a confrontation in the voting booth where someone challenged my candidate's choice, the choice of the candidate I wanted to vote for. Eventually they punched a hole in the ballot card, and I trusted that they punched the candidate that I wanted to select.

What I would like to share with the committee is our experience working with Sequoia Voting Systems. We selected a machine, the only verified paper ballot machine at the time in 1985 when we worked with Sequoia spending considerable resources, and they spent considerable resources. The disability resources elected officials, including Cook County organizations, spent considerable time, resources, and energy working together, as well as Sequoia, including the company president, meeting with disability leaders several times, and it resulted in significant advantages.

That access was quite substantial and significant. Dozens of changes were made. Two control boxes were produced during that time period, one for the primary election and one for the most recent general election.

So I guess my time is up, and I have submitted my written testimony.

Ms. LOFGREN. We thank you very much.
[The statement of Mr. Pierce follows:]

COMMENTS FOR THE HOUSE COMMITTEE
ON HOUSE ADMINISTRATION

Elections Subcommittee Hearing on Election Reform: Machines and Software

Delivered by:

Kelly Pierce

March 15, 2007

I Am Kelly Pierce the Disability Specialist at the Cook County Illinois State's Attorney's Office and a member of the Accessibility committees of the Cook County Clerk's Office and the Chicago Board of Election commissioners. I have worked on disability related technology and transit policy issues since the early 1990s. This included starting a technology user group for blind persons and consulting with the local transit agency on its audio interface for a new automatic stop announcement system. I have served on the Technology Watch committee of the National Council on Disability, a federal agency that plans and evaluates disability policy and programs. I have worked with major financial institutions including Bank One, J.P. Morgan-Chase, LaSalle Bank, and American Express in creating and developing audio interfaces to automatic teller machines for people with disabilities. More recently for the past two years, I have worked with Sequoia Voting Systems and the Cook County Clerk and the Chicago Board of Election Commissioners to develop significant improvements in accessibility to electronic voting machines in Cook County.

I became blind in 1985 at the age of 20 from a rare genetic eye condition, having voted in the 1984 election for the first time. Following my vision loss, I voted with the assistance from others until last year when I voted independently for the first time as a blind person. During those two decades, I endured humiliating and degrading privacy compromises, illiterate poll workers and arguments in the voting booth. Friends that assisted me sometimes revealed to others who I voted for. Once, a friend challenged my candidate selection and argued with me in the voting booth before casting a vote, for whom I still am not sure. Only once did I seek the assistance of election judges. One of the judges, an elderly woman, had difficulty seeing the print on the ballot and following a line to punch the right hole in the ballot card. The election judge she called over mispronounced most of the names on the ballot to the point many of them needed to be spelled. He also missed parts of the ballot and could barely read several referendum questions.

Last year, this all changed. I was able to vote independently for the first time. It was an exhilarating and awesome experience once again to feel with a high degree of confidence that my election choices would be received and fully counted as those of everyone else in my community. The experience was also highly satisfying. Two years ago today, on March 15, 2005, I reviewed four proposed election systems at the request of local election authorities, including the Cook County clerk. The resulting 100-page report found accessibility barriers with all four voting systems, with some having significant

barriers. In May 2005, the clerk chose the only direct-recording electronic voting machine that had produced a voter-verified paper audit trail in an actual election. While the Sequoia electronic voting system had significant accessibility problems, assurances were provided by the company's Chief Executive Officer to devote resources on dramatically improving access.

The company followed through on its commitment. On June 13, 2005, Sequoia Voting Systems then President and CEO Tracey Graham met with disability leaders and the Cook County Clerk and described the company's substantial commitment to improving the accessibility of the AVC Edge. An audio recording of a voting experience was produced that day following this meeting. The recording and end user experiences with the Sequoia AVC Edge were used to produce a June 30, 2005 report on the audio interface of the machine. Since completion of the report, Sequoia representatives spent more than 100 hours in enhancing and improving the audio script used by the AVC Edge, states a December 2005 memorandum by Sequoia President Jack Blaine. During the past two years, Mr. Blane has met with disability leaders to learn about access concerns and develop paths for forging solutions. City and county officials and leaders from the disability community spent hundreds of hours conducting usability tests, analyzing the control box, and reviewing the effectiveness of each audio prompt on the machine. Further, Sequoia redesigned its control box for the audio interface. The new control unit included easy to locate volume control buttons and a switch that increased or decreased the rate of speech in the audio recording. The new control unit also enabled those who could not use their hands to vote to plug in a sip and puff device so the ballot could be voted completely from someone's assistive technology.

Additionally, Sequoia produced numerous changes for the November 2006 election. In August 2006, Sequoia representatives met with the Cook County Clerk, the Executive Director of the Chicago Board of Election Commissioners and leaders in the disability community to demonstrate the new and enhanced accessibility features of the Sequoia Edge II Plus voting machine, which was used in the November 2006 election. The Sequoia Edge II Plus replaced the AVC Edge used in the March primary election. The audio interface now includes navigational prompts on the contest menu and an interactive ballot review mode so blind and disabled voters can exit the review mode at a particular contest and change their selection as sighted voters can. The now accessible ballot review will largely resolve the problems that were described in my report. The company may refine the accessibility of its ballot review, further increasing the accessibility and usability of this newly accessible function. The re-designed touch screen on the Edge II Plus has legs that can be adjusted to different levels for various wheelchair heights. For the first time, people who have low vision will be able to view the ballot using a zoom function which magnifies the type up to 400 percent its normal size as well as view the ballot at a high color contrast. Sequoia has re-designed its audio control unit yet again. The buttons are concave and recessed so those with head or mouth sticks and pointing devices can operate the machine independently. There are now also separate large plug-in "buddy buttons" for people with limited dexterity to use. I understand that many of our

improvements could easily be retrofitted to other Sequoia machines in the rest of the country.

This rapid and remarkable increase in accessibility did not happen by accident. It came about through a deliberate process when a government purchaser, as its largest customer, put forward clear access expectations. Also, Cook County Clerk David Orr and Lance Gough, the Executive Director of the Chicago Board of Elections, became personally involved in the process, actively pursuing effective accessibility as one of their important goals. Further, company management from the CEO on down became focused on access goals and talented and seasoned disability leaders along with company representatives devoted considerable time and resources innovating and creating powerful solutions. When representatives of industry, government and the disability community work together cooperatively as partners in using technology to solve accessibility problems, the inconceivable becomes possible enabling a new level of independence never before achieved.

Finally, I wish to comment upon legislation before this sub-committee, HR811 the Voter Confidence and Increased Accessibility Act of 2007. From my reading of this bill, it would require voting machines that produce paper ballots that can be hand counted. Further, the completed paper ballot would need to be able to be read back in audio to the voter with a disability. While the Sequoia electronic voting system has a voter verified paper audit trail, it does not have this functionality. This means that all of our new voting machines would need to be discarded along with the loss of time, energy, pride, and dreams of people with disabilities, and those in industry and government who created a highly effective access solution. Currently, there is only one voting machine that meets the requirements in the bill and this machine has access issues and barriers of its own. Access with technology for people with disabilities is not a simple either/or proposition. A wide range exists from the highly accessible to those devices that provide some minimal access features. The tremendous access achieved with our voting system should not be disregarded in an effort to further improve upon voting system improvement.

I am passionately looking forward to voting in next year's presidential election. It will be the first time me and other blind and disabled people can cast a vote for president privately and independently without needing to reveal the choice to friends, family or community members.

Ms. LOFGREN. Next I would like to ask Dr. Selker from the Voting Technology Project at MIT to share his thoughts with us.

STATEMENT OF TED SELKER

Mr. SELKER. Ladies and gentlemen of the committee, thank you so much for having me.

I have been working on voting technology since the 2000 election problems, and the goal of producing lost votes universally requires us to make selection accessibility, and you have to think about how the process has gone. It has always been that people are going back and forth between ballotless and balloted. Voting with ballotless, you are using a systematic control of some sort, some mechanism to check for problems, and with ballots you are using humans to control for problems.

To the extent that we have humans in the process, which we very much do, we have to have performance-based approaches to test the quality of every step of the process. And I think that during the ballot counting and recording, we are always in danger of losing ballots. And today 1 in 30 selections on every commercial system that I have tested is for the candidate next to the one you meant to vote for. It is worse if you have reading disabilities, and it is easy to make improvements with that. We have done it in the laboratory with systems that make them more readable, and you have better feedback and more redundancy.

The second chance approaches that we all are working towards with the Help America Vote Act include using VPACs, and what we have discovered in testing various approaches, that if you have people with optical scans try to verify, they don't find problems. If you have them with VPACs, they have 106 ballots with errors no one reported. You get a lot more with the audio. You get another almost six times more people reporting. Not everybody catches the problem, but people get more.

The thing we want to take care of is not to be adding to the problems we have. There are improvements that can be made to paper trails if we work towards it. But basically I guess what I really want to make sure that we are focusing on is that in the end, we are making sure that any record that we use is reliable enough to improve voting; 1 in 500,000 may be a good number for how often you don't want the equipment of the machines to stop you from voting.

What should be the best evidence if you have a problem? If you have two records, it should be that we know to look for the one that we are sure is good evidence and we can figure it out at the time.

My time is up.

Ms. LOFGREN. We appreciate that. We have your testimony.

[The statement of Mr. Selker follows:]

U.S. HOUSE ADMINISTRATION SUBCOMMITTEE ON ELECTIONS HEARING ON ACCESSIBILITY AND USABILITY—MARCH 15, 2007, 2 P.M.

TED SELKER, ASSOCIATE PROFESSOR, MIT MEDIA LAB, MIT DIRECTOR, CALTECH/MIT VOTING TECHNOLOGY PROJECT

Thank you for the honor of inviting me to give testimony to the House Administration Subcommittee on Elections, hearing on accessibility and usability. I want to thank the members of the committee for allowing me to testify.

I'm Ted Selker, Associate Professor of the MIT Media Lab, and co-director of the Caltech/MIT Voting Technology Project. I invite you to email me follow-up questions at Selker@Media.MIT.edu. I'll be talking about reducing lost votes universally. As we are trying to improve elections, we must use universal design to make selection accessibility possible for all voters. The process must be accurate. Systems have been developed which use ballots and have physical records which rely on human control. More recently, approaches have been developed with systematic ways of counting ballots with computers, or with mechanical systems. These systems, such as lever systems and electronic voting machines, depend on systematic mechanisms for testing the votes, and human control as back up. The process of reducing lost votes universally requires humans to use performance based approaches to test all parts of the vote. Secondary records might improve auditability but only if they are independently verified to be accurate and reliable.

Selection accessibility is the central problem for everyone, and especially for people with reading disabilities. All technologies that are used today lose votes. Typically with paper ballots and with electronic ballots, we see one mistake in thirty selections in which a voter selects the adjacent person, choosing a candidate that they did not mean to vote for. It is very easy to reduce these mistakes. We have made ballot designs and mechanisms that can reduce the errors of these sorts by fifty percent to eighty percent.

Elizabeth Rosenswieg, Anna Pandolfo and I created experiments which have compared voter verified paper trails, contemporaneous paper trails, optical scan voting, and audio verification. These experiments found that it is very difficult for people to notice mistakes. In experiments with over 30 voters, no one found an error. The voters who had a paper trail found their errors 30 percent of the time. With contemporaneous paper trails, 40 percent of people found their errors. However, they had 15 percent more errors than any other group. The act of having to pay attention to two things, the paper being printed out, and the electronic voting experiments, distracted them enough that they made extra errors. When using audio verification, 50 percent of the people found errors. In earlier experiments in Sharon Cohen's work, the audio found six times as many errors as the voter verified paper trail.

We are not saying that verification records that are produced with audio or paper are the only way to have second chance voting. Certainly the review panes can be an excellent possibility for getting people to do second chance voting as well. However, these have to be designed in a way that helps guide a person to notice when they have under voted.

In sightless voting we are especially concerned about selection accessibility. The audio ballot designs of today takes a sightless voter tens of minutes to complete. This has to be improved. The goal is access for people who have disabilities, not assistance. Up to 15 percent of the American public is reading disabled. Alignment improvements, simple layout, audio feedback, can all improve voting. The sight disabled can be helped with large ballots, large icons, words and buttons. High contrast and audio redundancy also helps them. People with other cognitive disabilities such as short-term memory problems, are helped by memory aids and audio feedback.

In addition, performance based election administration qualification is central to keeping votes from being lost. We cannot know that we've trained election administration personnel until they demonstrate that they can do the job. At every step in the process, we must have people that know how to independently corroborate each other's work in ballot counting, and reporting of the votes so that there is no change in the votes made by anybody but the voter.

Serious research has been done in all of these areas. We have made the low error voting interface for helping people with reading disabilities and with sight disabilities. It uses redundancy with tabs that allow a person to see all of the races and the status of all the races simultaneously, as sort of a review pane that is always on the page. It uses large changes in the contrasting coloring of the race to show that it has been made. It shows one race per pane, and it uses the idea of simple layout, redundant feedback, and collaborating information as principles. We've also worked on audio which replaces beeps with words to give redundant confirmation and reduce voting time. To aid unbiased selection, the sex of the audio speaker

should match the sex of the candidate that is being selected. Essentially, to improve ballots, the research has to be continued.

All forms of ballots must be evaluated before they are used. For example, we evaluated the ballot style used in Sarasota, Florida in 2006, and found that where there is an orphaned race on the same pane as another race, the residual rates increase substantially. In Charlotte County, Florida, the Attorney General race at the top of the ballot had a 22 percent under vote. And other races which are adjacent to it had less than 1½ percent under vote.

The goal is to focus on making legislation based on demonstrated systems that helps the system work. Can we make verification records that help even blind and disabled people improve their voting? So far the paper records have not demonstrated themselves to improve voting through verification, and in fact it appears that where they've been used, there is somewhere between 5 and 10 percent of them that are actually unreadable. Election process must strive to allow everyone to cast their intentions without mistakes.

Things can be improved, and we must use this research. Legislation should not determine ahead of time that paper is the official record. To keep a record from being a target of fraud one should decide which available evidence is valid for what purposes after they've been created, not before.

Records must be reliable, and whatever records we make must be able to comply with 2002 voting standards of one in 500,000 errors. We should not make legislation for technologies that have not been tested. We must specify systems that will improve reliability before we ask people to buy new systems. Purchasing equipment that is not tested wastes money in a time when we could be improving our elections to be a model for the world. I encourage you to consider the Policy piece from June 2005 Science Magazine I submitted, and I encourage you to view more information at *www.votingtechnologyproject.org.* Thank you for your time, and I submit my testimony to the official record.

Ms. LOFGREN. We are honored to have the secretary of state of Mississippi Mr. Clark come all the way up here and give us the benefit of his experience and wisdom.

STATEMENT OF ERIC CLARK

Mr. CLARK. I am delighted to be here. I appreciate having the opportunity to be here.

There are five points I want to try to make very quickly, and I think I can do it in 3 minutes. I am here as secretary of state of Mississippi and also as cochair of the Elections Committee of the National Association of Secretaries of State.

First as to the disability issues. Two years ago, I appointed a task force in our State to pick a State voting machine, and we wound up with 77 out of our 82 counties taking that machine, and counties could either opt in or opt out. Citizens with disabilities were very active in that task force and had an extremely important influence in helping us pick the machine. We picked a touch-screen, and they were among the most vocal supporters of it, and people have told me for the first time they are able to vote a secret ballot. Like a person who is not able to see, there is an audio feature that walks that person through the ballot. It is extremely successful.

I will tell you that not only the disability community, but generally, the machines are very, very popular in my State. It is more than a 98 percent approval rating in the surveys we have done. So we are in good shape there.

I would ask you this: Please don't break something that is working; but if you do, please, please, please give the States enough money to fix it. Now, where we are is the only bill I have seen introduced talks about $300 million. That won't begin to do what that bill would mandate on the States. And I say that within the context that HAVA was underfunded to $800 million. So please don't make us do something we can't afford to do.

If I may touch on three other issues.

We have a paper trail in Mississippi. We bought a printer for every one of our DRE machines that is State involved. They work very well. They use thermal paper. It has a life of at least 5 years. The main—H.R. 81, that is the bill that I read, would make us do away with that. I think that it would be completely unnecessary, and I think it would be a complete waste of a lot of folks' time and money. It says a paper trail has to be on durable paper of archival quality capable of withstanding multiple counts and recounts, without compromising the fundamental integrity of the ballots. If you take out the word "durable," because I don't know what a court would say that means, and if you take out "of archival quality," our paper trail right now meets that test.

The second point, it says the auditor has to do recounts. Please don't give that function to somebody that knows nothing about elections, somebody who would simply complicate the process and make it impossible for us to certify the elections timely. My auditor is very much against it, and there is a letter from the National State Auditors Association saying that is a bad idea. Please give the folks with the responsible authority the opportunity to do their job.

And the fifth point is please don't make us do that this year. That is what the bill says. We have 4 years to implement HAVA. There is no way under the sun we can make the kind of changes that are contemplated in that bill by next year's elections.

I have gone 12 seconds over. Bless your heart. Thank you for listening to me.

[The statement of Mr. Clark follows:]

Testimony of
Eric Clark, Mississippi Secretary of State
Before United States House of Representatives
Committee on Administration
March 15, 2007

Ladies and Gentlemen of the Committee, thank you for inviting me to testify before you today concerning voting systems, disability access, and more proposed changes to our nation's election systems through federal legislation. These issues were the subject of much discussion during several sessions at the winter conference of the National Association of the Secretaries of State (NASS) held recently here in Washington. I have been asked to focus specifically on issues related to disabled citizens, which I am happy to do. With your permission, I will also take this opportunity to speak briefly about more general concerns which we secretaries of state have concerning proposed legislation in your Committee. I serve as co-chair of the NASS Elections Committee. Many secretaries of state, including me, are deeply concerned about some of the proposals being discussed in Congress.

In Mississippi, two counties used touch screen machines prior to the adoption of the Help America Vote Act of 2002 (HAVA). Since passage of HAVA, 77 out of the 80 remaining counties have acquired touch screen voting machines with a voter verified paper audit trail. We have expended nearly $16 million dollars to purchase new voting equipment in compliance with the goals of HAVA. This amount includes $6 million in state funds which our Legislature provided last year, because third-year funding of $800 million as authorized by HAVA was not appropriated by Congress. Now Congress appears to be poised to change the rules again and require the purchase of new voting equipment, some of which has not even been thoroughly developed, at tremendous costs to the states.

As reported recently in a CNN poll discussed at the NASS conference, more than 90 percent of the public likes the new voting equipment purchased in response to HAVA. According to a thorough survey done in Mississippi following our 2006 elections, 89.7 percent of our citizens said they found the new voting machines to be easy to use. To put it bluntly, in Mississippi, as in most of the country, the people have overwhelmingly accepted the new voting equipment and have confidence in it. Why destroy this confidence through new federal mandates?

In Mississippi, we decided to go with the touch screen voting machines for a variety of reasons, and one important reason was the accessibility of this equipment for disabled citizens. I appointed a task force which included citizens with disabilities, and their input weighed heavily on the selection of our new voting machines. We did not take the decision to spend $16 million lightly. Ease of use for the voters, accuracy and accessibility were key factors we considered when purchasing this equipment. The disability community in our state is among the strongest supporters of our new voting machines. In particular, blind persons are able, through audio directions, to vote a secret ballot for the first time ever. Because we heard from the public that voter verified paper audit trails or VVPAT would give them more confidence in the system, our machines were purchased with this feature. Much of the conversation about touch-screen voting in Washington seems to overlook the ease of use factor for voters generally and especially for citizens with disabilities.

While well intended, legislation proposed to again change the voting systems has several major flaws. First and foremost, it would place enormous new federal mandates on the states for the 2008 elections in the areas of voting equipment and procedures without providing sufficient funds to make the required changes. The most money we have seen in any draft bill is $300 million to implement equipment mandates. However, state election officials across the nation recognize that this sum is much less than what would be needed to accomplish the overly ambitious task.

Several specific requirements contained in proposed legislation regarding voting systems are ill conceived. Among the mandates proposed are:

- Requiring all voter verified paper audit trails to be accessible to disabled voters – even though such equipment currently does not exist. It defies logic that we would required to add a component to an election system for an election year, not to mention a Presidential election year, when that component has not been developed, tested, piloted and manufactured.

- Another mandate seems to require that each voting precinct have more than one voting machine. This is a suggested best practice issued by my office to our county election officials, but it has not been mandated to our cash strapped counties, especially with the federal shortfall in HAVA funding.

- Proposed federal legislation also mandates that the paper used for the voter verified paper trail be "durable paper of archival quality capable of withstanding multiple counts and recounts without compromising the fundamental integrity of the ballots." Mississippi bought the voter verified paper trail printer for all of the state-purchased voting machines. These printers use thermal paper which has proven to provide a high quality print, is inexpensive, easy to use, and lasts a minimum of five years. The language quoted above would require our counties to discontinue the use of this paper. Let me say that if the provision I just mentioned were amended to delete "durable" and "of archival quality," I believe all of Mississippi's 82 counties except two would qualify at the present time. **If Congress decides to mandate a voter-verifiable paper audit trail on all voting machines, please do not destroy the actions already taken by states that have successfully met that goal, at enormous expense, and require us – unnecessarily – to start over.**

Please allow me to mention one other serious problem with legislation that has been introduced in this Committee. I understand that this Committee will hold a hearing next week on the issue of post-election audits. Since I will not be here then, may I briefly address that topic now? I believe I speak for every secretary of state in the nation in expressing this concern.

Astonishingly, language has been proposed that would create a new level of state bureaucracy by mandating that the state auditor appoint an "Election Audit Board" which is required to go into selected counties to conduct thorough hand recounts of ballots in conformity with a detailed, mandated process. Furthermore, proposed legislation would prohibit any state or local election official – someone who might actually understand the election equipment and the election process – from serving on the Audit Board or conducting these hand recounts. It must also be pointed out that these federally required recounts must occur within a very narrow window, which could potentially impair the certification of election results within the time frame required by state law. Bringing a separate elected official into the process who has no role and no experience in conducting elections would make concluding our elections enormously more difficult and time-consuming – and possibly politicized -- and would be unwise almost beyond belief.

I want to emphasize at this juncture another critical problem with the proposed changes – all of these new federal election mandates would be required to be implemented by the 2008 federal elections. This would give the states less than one year prior to the first primaries to put into place massive changes in equipment and procedures. Congress wisely gave the states four years to implement HAVA. A further overhaul in our elections should be given at least that much time to find the proper contractors for new voting systems and change state laws to conform with any new mandates imposed by Congress.

Continued federal involvement by legislation means also seriously erodes the sovereignty of the states over elections issues, a bedrock principle of our democracy since our nation's founding. As you know, when it comes to elections, one size does not fit all. What works well in a state like New Hampshire, with its unique New England character and conventions, is often inapplicable to Mississippi, with our distinctive history and makeup. The states must have the flexibility to tailor our elections equipment and procedures to our citizens' desires and needs. Indeed, one of the best aspects of HAVA was the fact that it recognized and embraced this core canon – HAVA mandated certain key goals but left it to the states to determine the best means – both in terms of voting equipment and voting procedures – to achieve those goals. Proposed legislation that we have seen would deviate from this proven formula for success by mandating specifically the equipment and the procedures which the states must use.

Finally, all the proposed legislation has been drafted in a vacuum or at least without input from election officials. No input was requested from NASS or from any of the state election officials. This is incredible! My colleagues at the state and local level are election administration experts. Why not ask the people who run our elections, who know the nuts and bolts, who see what goes on at a local level, and who must deal with the implementation of any new federal requirements, to have a say in this process?

I urge you in the strongest possible terms to reconsider the proposed legislation, or to amend it to answer the concerns expressed above and to make sure that there is adequate funding to pay for any new federal mandates.

In conclusion, the whole elections community in Mississippi - circuit clerks, election commissioners, disability groups, party officials, and the secretary of state's office - has worked extremely hard and effectively in a bipartisan manner to implement the Help America Vote Act of 2002. Representatives of the federal Elections Assistance Commission and the United States Department of Justice have repeatedly, publicly held Mississippi up as a good example of how to do HAVA well. Many other states have made similar progress. Please do not come along now and tear down the enormous progress we have made.

Thank you for your consideration and your attention.

Ms. LOFGREN. I will ask unanimous consent to put the letter into the record.

[The information follows:]

National State Auditors Association

EXECUTIVE COMMITTEE

President
ERNEST A. ALMONTE
Auditor General
Rhode Island

President-Elect
BRUCE A. MYERS
Legislative Auditor
Maryland

Secretary/Treasurer
RUSSELL W. HINTON
State Auditor
Georgia

Immediate Past President
AUSTON G. JOHNSON
State Auditor
Utah

DEBBIE DAVENPORT
Auditor General
Arizona

PHIL BRYANT
State Auditor
Mississippi

ALTER J. KUCHARSKI
Auditor of Public Accounts
Virginia

NASACT EXECUTIVE DIRECTOR

R. KINNEY POYNTER
Lexington, Kentucky

CONTACT INFORMATION

Headquarters Office
449 Lewis Hargett Circle
Suite 290
Lexington, KY 40503-3590
(859) 276-1147
Fax (859) 276-0507

Washington Office
444 N. Capitol Street, NW
Suite 234
Washington, DC 20001
(202) 624-5451
Fax (202) 624-5473

www.nasact.org

March 08, 2007

The Honorable Rush Holt
United States House of Representatives
Washington, DC 20515

Dear Representative Holt:

On behalf of the National State Auditors Association (NSAA), I am writing to bring to your attention a provision in HR 811, the *Voter Confidence and Increased Accessibility Act of 2007*, which could be perceived as a conflict of interest for the state audit community and, in some circumstances, could create a perceived independence issue for state auditors.

Section 321(a) of the bill states that the Election Audit Board and mandatory manual audits of paper ballots would apply to "each election for Federal office held in the state" and "at the option of the state or jurisdiction involved, of elections for state and local office held at the same time as such election." It is this latter provision (applicability to state and local elections) that causes concern for **elected** state auditors. Under this provision, the Election Audit Board could be verifying the ballots of an elected state auditor, the same person who appointed the members of the Board. This creates an independence impairment as outlined in *Government Auditing Standards* issued by the Comptroller General of the United States.

We are similarly concerned with Section 321(d) which defines 'chief auditor.' The definition allows the attorney general of the state to designate and certify the chief auditor. In some states, there are two individuals that would qualify as auditing the operations of the state government. Some states do not use specific constitutional or statutory language to define the duties and responsibilities of their auditors, which also raises the questions of who the attorney general will designate and certify as the chief auditor. In addition to this concern, a conflict of interest could exist as the Election Audit Board could be verifying the ballots of an elected attorney general, who ultimately is the person designating the "chief auditor" to appoint members to the Election Audit Board.

Furthermore, it would be very difficult -if not impossible- for a state audit office to preserve its independence for the core function of auditing state government as is required under the independence standards in *Government Auditing Standards*. State audit offices are generally non-partisan having no interaction - in either professional or personal capacities - with political parties. To the extent that the proposed Election Audit Board would consist of political appointees as well as "unaffiliated members" appointed by the chief auditor, the opportunity for political influences would exist. Additionally, the pool of individuals qualified as "unaffiliated members" for appointment to the Election Audit Board is inherently limited. While employees of a state audit office would be qualified, such service would deviate from the duties those individuals are paid to perform. Staff of

private accounting firms may qualify, however, the state audit office often contracts with such firms to perform (in many instances by state statute) auditing of state agencies and, for independence purposes, the audit office does not have any other relationship with such private accounting firms. State agency employees may qualify to serve on the Election Audit Board however a state auditor's independence to audit them in their routine state capacities could be called into question by virtue of the state auditor appointing those individuals to serve on this new Board.

Lastly, we do not believe the state auditor is the appropriate person to be given such appointment responsibilities. While we understand the need for such audits, the responsibility for these audits seems to be an internal control/internal audit matter. Establishing internal control is not the purpose of the external audit function; rather, it is management's responsibility to establish and monitor internal control. We believe the audit function as outlined in the bill should be internal to a state agency, such as the state board of elections or other similar type agency.

We look forward to working with your staff to amend the bill's language to address these issues. Should you have additional questions or desire further information, please contact NSAA association manager, Sherri Rowland (srowland@nasact.org or 859-276-1147) or NSAA Washington director, Cornelia Chebinou (cchebinou@nasact.org or 202-624-5451).

Sincerely,

Ernest A. Almonte
Auditor General, Rhode Island
NSAA President

Ms. LOFGREN. And we also have a letter from a number of disability activists that I will also ask unanimous consent to put in the record before we call on our next witness.

[The information follows:]

Americans with Disabilities Call for Election Systems Featuring Both Accessibility and Security

Voters with disabilities, sensory impairments, and special language needs have long been disenfranchised in large numbers as a result of lack of access to the voting process. For many of us, the passage of the Help America Vote Act of 2002 held tremendous hope and promise for secure and reliable voting, a guarantee that every voter would have access to the voting process.

Electronic ballot systems such as the direct record electronic (DRE) machines (formerly called "touch screens") now in use have quickly proven to be neither fully accessible to all voters nor secure and accurate methods of recording, tallying, and reporting votes. While the goal of private voting has been achieved by some voters, this has often been without meaningful assurance that our votes have been counted as cast. Additionally, many other voters have been disappointed and frustrated because we have not been able to vote privately and independently as we had hoped and as voting-system vendors had promised.

It is now clear that in order to guarantee reliability and security in our elections, it is necessary for the voter to be able to truly verify the accuracy of his or her ballot--the ballot that will actually be counted. The only voting systems that permit truly accessible verification of the paper ballot are ballot marking devices. These non-tabulating devices, either electronic or non-electronic, assist the voter in marking and verifying votes on paper ballots that can either be optically scanned or hand-counted. (Some DRE voting machines that have already been purchased may be adapted to be used as acceptable ballot marking devices, assuming their accessibility can be preserved or improved.)

The technology for inexpensively providing good accessibility to voting systems has been commonly available for more than a decade, and it can and should immediately be required for and applied to all modern voting systems.

This is clearly illustrated by the report "Improving Access to Voting: A report on the Technology for Accessible Voting Systems," by Noel Runyan, posted at VoterAction.org and Demos.org. Design of new systems must include, from the beginning, accommodations to allow private and independent voting by individuals with a broad range of access needs. These systems must simultaneously ensure secure elections.

We leaders and members of the disability rights community assert that neither accessibility for all voters nor the security of the vote can be sacrificed for the sake of the other. Fortunately, true accessibility and election security can both be achieved; there is no inherent incompatibility between voting system accessibility and security.

We recognize that electronic ballot systems are inappropriate for use, because these systems make it impossible for voters to verify that their votes will be counted as cast. We call upon all disability rights groups, other civil rights groups, election protection groups, and elected officials to recognize the necessity for an immediate ban on any voting system that fails to meet the twin requirements of full accessibility and election security.

List of signatories as of 3/14/07 (affiliations are listed for identification purposes only):

Noel Runyan, Voting access technology engineer and author of "Improving Access to Voting"

Roger Petersen, member, Santa Clara County Advisory Commission for Persons with Disabilities and Santa Clara County Voter Access Advisory Committee

Bernice Kandarian, President, Council of Citizens with Low Vision International

Robert Kerr, ACB Maryland

Shawn Casey O'Brien, KPFA-FM in Los Angeles, and California Secretary of State's Ad Hoc Touch Screen Task Force member

Suzanne Erb, Chairperson of the Philadelphia Mayor's Commission on Disabilities

Mike Keithley

A. J. Devies, Past President, Handicapped Adults of Volusia County (HAVOC); Charter Member, Daytona Beach Mayor's Alliance for Persons with Disabilities; Disability Consultant and Board Member, Florida Fair Elections Coalition

Marta Russell, independent journalist and author

Judith K. Barnes, Life Member, Council of Citizens With Low Vision; Former President, Silicon Valley Council of the Blind

George Moore, Accessibility Advocate, Californians for Disability Rights

Mike May, President, Sendero Group

Margaret Keith, VP, Monterey Co. Chapter, Californians for Disability Rights

Adrienne Lauby, Host/Producer, Pushing Limits, disability program on KPFA fm

David Andrews

Jean Stewart, Writer

Ruthanne Shpiner, Pushing Limits Radio 94.1 FM, Northern California ADAPT

Mike Godino, President, American Council of the Blind of New York, Systems Advocate, Suffolk Independent Living Organization

Louis Herrera

Dawn Wilcox, BSN RN, Past President Silicon Valley Council of the Blind, Board member CCCLV

Ms. LOFGREN. Our next witness is Diane Golden.

Dr. Golden, thank you so much for being here.

STATEMENT OF DIANE CORDRY GOLDEN

Ms. GOLDEN. Thank you. I am so impressed with how quickly somebody from Mississippi talks, because I talk really slowly, and I thought that is okay. Somebody before me is going to talk slowly. That isn't the case. I will quickly try to summarize my comments.

Thank you for inviting me to testify. I am very pleased to be here. First off, I am not here to oppose or endorse any voting system. I am here to talk solely about accessibility, which is what I know, love, and have done for the last 30 years.

Accessibility in voting systems is no different from accessibility to computers or telephones or any other types of equipment that you provide accessibility to people with disabilities. It means you have a set of access standards, and the equipment or the device conforms to those standards. That is how you judge whether or not something is accessible. If indeed the decision is made that one or more of the determinative votes of records needs to be paper, then that paper needs to be accessible, period. There is just no two ways around it. It is not going to work to have an accessible electronic vote record or ballot and an inaccessible paper one. You just see the problem with that. It is clearly lack of equal access.

So the good news is we have, I think, a very good set of access standards in the voluntary voting system standards that the EAC adopted. They are fairly robust. They could be improved, but they provide a wide range of access features for people who are blind, people who have low vision, people with motor limitations, et cetera. So it is a cross-disability way of delivering access.

The down side is that when you add paper into that process, we currently don't have equipment on the market readily available that delivers all of those access features when a paper ballot is involved.

And I will tell you just very quickly the two major access problems we have. The DRE systems that are on the market with the VVPAT attached, as Mississippi is using, the problem with accessing those systems is that the print on the paper is not accessible. That print is going to have to be converted into an accessible form for people with disabilities to actually be able to verify the paper. Currently what they are verifying is the electronic ballot.

The second equipment on the market are ballot-marking devices where the vote starts and ends paper, but there is an electronic interface that lets the person with the disability use large print, audio, switches so that they don't have to touch or handle anything. Those systems are fully accessible except for the fact that you have this paper ballot that has to be sucked in, pulled out and physically manipulated, and for someone who is a quadriplegic, who has no use of their hands, it is impossible. So again, you have lost independent voting ability.

So those are the two major access barriers we have when you reintroduce or mandate paper in the process. Are those two issues insurmountable technologically? No. They certainly can be addressed and resolved. What will it take? Time and money. And I will echo the secretary of state's statement: It is going to take us time and

money, but it can be done, and if that is what needs to be done to make voting secure, so be it. We just need to make it accessible at the same time.

Thank you.

[The statement of Ms. Golden follows:]

Testimony before the Committee on House Administration
Elections Subcommittee Hearing on Election Reform: Machines and Software
March 15, 2007

Presented by
Diane Cordry Golden, Ph.D.
Director, Missouri Assistive Technology

Madame Chair and members of the committee, thank you for the invitation to testify today. My name is Diane Golden and I currently work as the Director of Missouri Assistive Technology, the congressionally mandated statewide program in Missouri that provides a wide range of assistive technologies, including computer adaptations, for individuals with all types of disabilities. In addition to program administration duties, I serve on the Board of the national Association of Assistive Technology Act Programs and provide technical support to the National Disability Rights Network on voting equipment access issues. I have also provided invited testimony to the Election Assistance Commission (EAC) and the Technical Guidelines Development Committee (TGDC) on accessible voting systems.

Congress has recognized the need for specialized expertise in assistive technology by funding State Assistive Technology Programs in the 56 states and territories. These programs are required to address the assistive technology needs of individuals with all types of disabilities. A multitude of other federally funded programs focus on unique aspects of assistive technology and specific populations of individuals with disabilities. Historically in the discussions surrounding voting security and how to ensure accessibility, assistive technology expertise has not been effectively utilized. Individuals with unbiased knowledge and expertise in assistive technology were not typically involved in discussions regarding voting security even though many of the proposed solutions impacted accessibility.

As a preface to these comments, I want to emphasize that the disability community shares the interest of all Americans in ensuring that elections are fair, secure and accurate. From a personal perspective, I do not support or oppose a requirement for paper ballots as necessary to ensure security nor do I want to outlaw or promote any particular voting system. My expertise and focus is on accessibility. To that end, I am here today to discuss accessible voting under the Help America Vote Act (HAVA) and proposed verification legislation. In considering these issues, the following three points are critical:

1) The determination of whether or not a voting system, with or without a paper ballot, is "accessible" (and therefore meets any legal requirements to be "accessible") should be based on conformance to a set of nationally accepted technical access standards. Such determinations should not be based on individual anecdotal experiences.

2) If the decision is made to require a paper ballot, as a determinative vote of record, that paper ballot should be accessible, i.e. conform to an accepted set of access standards.

3) A robust testing process should be in place to verify that a voting system conforms to accepted access standards. The entity performing such testing must have comprehensive knowledge and understanding of accessibility features along with expertise and experience in assistive technology.

Status of Accessibility Standards and Conformance

The adoption of access standards as part of the Voluntary Voting System Guidelines (VVSG) required by HAVA has provided much needed direction regarding what is and is not considered to be "accessible." These access standards provide technical specifications regarding the access features that must be provided by a voting system for it to be considered an accessible system pursuant to HAVA requirements.

For example, the VVSG indicates that an accessible voting system must provide –

- An audio-tactile interface so that a blind voter can listen to the ballot and navigate/mark the ballot through tactile controls;
- Enlarged and enhanced text for individuals who have vision loss but cannot use an audio ballot;
- Simultaneous audio and enhanced visual display for individuals who have vision loss and those with print disabilities such as dyslexia; and
- A "non-manual" input option (usually dual switch) that allows individuals with very limited motor skills navigate/mark the ballot.

In reviewing products over the past several years, it appears that most of the access features required by the VVSG (excluding those related to accessibility of paper ballots) are being delivered by one or more direct response electronic (DRE) systems or ballot marking devices (BMD) with an electronic interface currently on the market. Features not currently available on existing products could be readily added as part of a redesign of the electronic interface of a DRE or BMD system. These electronic interfaces (absent paper ballots) that conform to the VVSG access standards deliver a wide range of access features that allow individuals with a variety of disabilities to vote secretly and independently, like all other Americans. As a result, many Americans with disabilities have enjoyed a certain level of accessibility in voting for the first time in their lives.

The Paper Challenge

If paper ballots are used to ensure security, those paper ballots must also be accessible to ensure the security of the entire election system and to uphold the rights of voters with disabilities to generate, verify and cast their vote privately and independently. Unfortunately, providing the same range of accessibility for a paper ballot, as is readily available with an electronic interface, is a bit more challenging, though not impossible. Two major shortcomings exist in current voting systems that use a paper ballot.

1) Direct electronic voting systems with voter verified paper audit trail (VVPAT) printers do not provide a mechanism for alternative access to the print on the VVPAT. As a result, voters with vision disabilities cannot verify the paper ballot privately or independently.

2) Ballot marking devices require voters with disabilities to manually handle paper to verify and cast their ballot. As a result, voters with motor and other disabilities cannot verify or cast the paper ballot independently.

The VVSG requires that systems utilizing a voter verified paper ballot as a determinative vote of record ensure that the paper ballot itself (not the electronic ballot) is accessible to voters with vision disabilities. The VVSG also requires that voters with motor disabilities be able to submit/cast the paper ballot without assistance. This means –

- Voters with disabilities should not be required to handle a paper ballot at any point in the voting process;
- Blind voters should be able to generate their vote using an audio-tactile interface and then should be able to verify/edit and cast the content of the paper ballot using that same interface;
- Voters with low vision who used enhanced visual display on the screen of a voting system to generate their vote should have enhanced visual display available to verify/edit and cast the paper ballot; and
- Voters with motor limitations who used switch input (e.g. sip and puff) to generate their vote should be able to use that same switch input to verify/edit and cast the paper ballot.

The most likely option for addressing access barriers in a DRE with VVPAT will be the utilization of a fixed scanner capable of automatically converting the human readable text of the VVPAT into electronic text. That electronic text can then be used to generate audio/speech output (through text-to-speech software or other mechanism used by the core DRE system) and enhanced visual display (on the visual display of the DRE.) The base DRE system will already have the capacity to deliver audio/speech output and enhanced visual display as it does for an electronic vote record. The same output mechanisms can be used, but will be based on the scanned content of the VVPAT, instead of the content of the electronic ballot.

The most likely option for addressing access barriers in a BMD will be the addition of an automatic paper handling mechanism. If the paper ballot can be manually fed into the system prior to beginning the vote process, and from that point on all paper handling is done via automatic feeding mechanisms, the access barrier will be eliminated.

While this all sounds complex, the technology to make this happen is currently available and can be developed if manufactures are given adequate time and guidance.

Independent Testing Labs

Testing entities entrusted with verifying voting system conformance to the access standards must have adequate knowledge and understanding of accessibility to do the job.
While the EAC has taken dramatic steps to improve the independent testing process for voting equipment, it is unclear what expertise and experience the testing labs have to adequately ensure compliance with the accessibility standards. Based on past experience with these same entities, it did not appear as if sufficient expertise existed to appropriately judge conformance to access standards. Time and time again, it was discovered that systems certified as conforming to existing Federal Election Commission access standards, in fact did not conform.

Summary

If Congress determines that in order to secure the voting process every voter must be able to verify and cast a paper ballot -- then *all* voters must be able to verify and cast paper ballots for our elections to be truly be secure. Moreover, verification measures must safeguard the rights voters with disabilities gained under HAVA and must allow all voters to verify their ballot privately and independently. A new access barrier should not be created by the addition of a verification requirement. Congress should not develop election access requirements to accommodate equipment vendors or the status of currently available voting products. Accessible verification technology will only develop if the law clearly requires it, and the technology will only be adequate if reasonable time and appropriate resources are allocated to support that development.

Ms. LOFGREN. Thank you very much to all of you.

We have been joined by the Chairwoman of the full committee, and we welcome her along with the other Members. Because we started so late, through no fault of our own, I am going to ask the Members to try to limit themselves to 3 minutes as well so that we will have time for the second panel. And I would like to start, if I can with Dr. Selker.

I understand that you have been a proponent of a voter-verified audio audit trail. Next week we are going to deal with auditing, but can you explain how that would work?

Mr. SELKER. Today's voting machines, electronic voting machines, have audio output, and if you simply had that go into a $50 tape recorder that tape records when there is noise coming into it, and from there into your ears, you are getting a verification record that did not go through a computer. It is not produced by—independently of you hearing it. And if it happens while you are voting, it actually helps people with disabilities because it corroborates the information that you are seeing, helping people with reading disabilities, helping people with cognitive disabilities of other sorts, and also it turns out that people find the errors, and that is what we like about it.

So now you take that tape, and the tape drive is a much more reliable drive than any of the printers that we have been able to find.

Ms. LOFGREN. Mr. Clark, I was interested in your testimony on how satisfied your State has been with the thermal ballots and your desire to make sure that what works for you is not disturbed, if I can put words in your mouth.

We had a hearing in the 109th Congress where we got a very different point of view from Ohio that has, I think, the same system with thermal paper, and they showed us things that were all jammed up and that didn't work.

Do you know—have you been lucky, or have they done something wrong, or do you have any idea why there has been such a disparate experience between the two States?

Mr. CLARK. No, ma'am, I don't. I can tell you what we have done in Mississippi. Last year we rolled them out in the early part of the year. We had primaries in June, and we had the general election in November. My staff in the Secretary of State's Office did more than 1,200 training sessions all over the State, in every corner of the State. And then, of course, we trained the county election officials, and they went out and did hundreds and hundreds of more demonstrations.

Education is at least 90 percent of the fight. And so we had hundreds of folks or actually thousands of folks, considering all the poll workers who worked hard to get prepared, and our experience was quite good.

In terms of problems, the first day we had an election, which was last June, in our primary, of our 77 counties that use the DREs for the very first time, there were problems in two counties because a technician set them up incorrectly, and it took us a few hours to get that fixed. But other than that, it worked quite well.

And I will tell you that the folks who, in my opinion, liked them best are retired citizens, and those are the folks who tend to have

indigestion, in my experience, because they are just a little bit suspicious a lot ahead of time. But after they have done it one time, they love them. So I think simply education is the key.

Ms. LOFGREN. I am going to set an example and stop questioning with 26 seconds to go and ask our Ranking Member Mr. McCarthy if he has questions.

Mr. MCCARTHY. First of all, I will just go right back to the secretary of state, Mr. Eric Clark.

A couple of things you stated. You talked about time line. You talked about the dollar amount not being enough, and you are referring to the bill which is now before us. I want to make sure that is correct what I was hearing from you. And you said you had 77 out of the 80 that used the touch screen, and they found it very supportive.

Mr. CLARK. That is right. Our experience has been very positive. I don't want to take too much of your time. We have 82 counties in Mississippi. Two of them had already bought touch-screen voting machines with their own money pre-HAVA, and those machines don't have a paper trail, a voter-verifiable paper audit trail. But then of the remaining 80 counties, our legislation said counties can opt in and take the State-purchased machine, or they can opt out and get their own, buy their own machine by their own manner. Seventy-seven of our eighty remaining counties opted in. And our experience last year, rolling them out first election, was extremely positive.

Mr. MCCARTHY. CRS has a new report out this month saying most county election officials are happy with the systems they have, but are unhappy with the systems they don't have.

If I could ask Diane, I found your testimony very interesting, and I need a little more explanation. Were you saying for accessibility, those that use DRE and added on the VPAT, the VPAT was not working, the paper for accessibility, and when was that? Can you give me a few examples of where it is used?

Ms. GOLDEN. The core DRE system is all electronic. So the voter interacts with it electronically, and it is stored electronically. All of that can be fully accessible because things that are electronic are easy to manipulate. So text can go to audio, text can be enlarged, I can use switch input.

What happened when paper got added onto the end of the electronic is then there is print on a piece of paper attached to the side of this machine, and no longer can the person with the disability see it to verify it.

Mr. MCCARTHY. Do you know of any technology that could?

Ms. GOLDEN. Scan it back in. That is what needs to happen. There needs to be some sort of a fixed scanner. The most direct, simplest solution—and not to argue with if there are better independent verification techniques, there absolutely could be, but if you are going to take what is out there now and try to add onto it again to make it accessible, there needs to be a fixed scanner so that the text that comes off that printer can be scanned, sent back to the electronic interface, and then however I marked it originally, however I read it originally, audio, large print, I am using switches to verify it, finally cast it; all of those interfaces are available to me.

Mr. MCCARTHY. Is that technology out there today?

Ms. GOLDEN. Sure.

Mr. MCCARTHY. Do you have any cost estimates?

Ms. GOLDEN. Not right now. It is building it into—you have a voting system that the printer was added onto. Now you are adding onto the add-on. So it is just in a research and development perspective. It is not the way you want to go about doing something because you are adding onto adding on.

Mr. MCCARTHY. Is anyone selling this product?

Ms. GOLDEN. The only systems out there that use scanners are scanning a bar code. So the printer that has been attached—or, for example, if you are familiar with the vote by phone system, it is an audio interface. I am voting by phone. It prints a ballot that also has a bar code on it, and there is an eyeball scanner. The vote ballot drops into a basket or box, the eyeball scanner scans the bar code, the bar code then comes back to me auditorily. So it is reading the bar code on the paper. It is not reading the human readable print on the paper.

Mr. MCCARTHY. Sorry. Time is up.

Ms. LOFGREN. Madam Chairman.

The CHAIRWOMAN. Thank you. Thank you for convening this important hearing today. We welcome you as our new Chairperson, but this is a very important hearing. Just this morning we had, I guess, about eight vendors demonstrating and displaying their wares on voting machines, and there was one who said he had the perfect voting machine.

Ms. LOFGREN. Just one?

The CHAIRWOMAN. At least he was arrogant enough to say that.

But getting to voting machines, we know that that is really the issue here with reference to voters, knowing that when they cast the vote, the vote will count, and it will be accurate and secure.

Ms. Golden, assuming that voter-verified paper ballots will be required in 2008, and let me ask each of you, do you think that we will be ready for a mandate for paper ballots required, verified paper ballots required in 2008, paper trails?

Ms. GOLDEN. I could answer really quickly in terms of the accessibility piece. No. It is just an awfully short time line to try to fix the two access problems that we still have in existing products related to print.

Mr. SELKER. In my experience, the paper trails have not been reliable, and they have not been verifiable nor accountable. As soon as we get good equipment that makes better records, makes records that actually improve elections, that is a great thing to have a better second-chance voting approach.

Today I watch as, you know, optical scan ballots are taken into back rooms to be counted. I watch as paper trails, printers are opened up to be fixed during the day. I mean, I personally watched these things. And I think that we have to first make these things work and show that they actually can find the problems that people have.

The CHAIRWOMAN. Let me ask you, you said you do not think paper trails are reliable. Is that what you said? And yet how do you convince the voter that they are not reliable? They tend to think

that this is it. If you don't have it, there is no point in going to the voting booth because their vote is not going to count.

Mr. SELKER. I watched in Nevada when they rolled out the first paper trails throughout the State, and one of the first polling places I went to, a guy came out of the booth and he started stammering, "But how do I know that my vote counted? There is no paper trail." and he had just—he had just experienced the first paper trail roll-out throughout a State.

So the advocates have been extremely good at getting people to get the rhetoric. The question is when people experience it, will they believe they are even experiencing it? You will see over and over again people trying to open the paper trail printers because the word "receipt" used to be used. So they think they will get a receipt, when, in fact, there is going to be a record that is going to, hopefully, be held safe and sound in the balloting.

The CHAIRWOMAN. My time is up already.

Ms. LOFGREN. We have our colleague from California Susan Davis.

Mrs. DAVIS. Thank you. I appreciate your all being here.

As we sit and talk about these issues, you feel like you are at the grocery store. Paper or plastic. And whether we can—and I am just wondering whether you think there is common ground on that issue; specifically that we could be or should be focusing on that perhaps has not been addressed, because people either feel comfortable with scanner ballots or with the DRE, and I am wondering where do you think that common ground is?

Mr. CLARK. My response would be that in terms of voter confidence, and I think that is what you are asking about. My experience in Mississippi has been extremely positive. We did the rollouts of the DREs with the voter-verifiable paper trail in the middle of the national debate—except "debate" is too nice of a word—in the middle of the national hoopla about this very issue, and the machines worked well. And the fact that we had the paper trail gave voters the confidence that their vote was being counted.

If I am—if you would indulge me for just a moment. There is a fundamental flaw in the logic of this debate; that is, there seems to be a sense that somewhere back in the past, there was a system that worked better, and I can guarantee you there was not. The machines that we have in Mississippi now are by far more accurate than anything that we have ever had before or that has ever existed before. And so the election is more accurate than elections have ever been. Just a few years ago it was not uncommon to have, in some cases, 15, 18 percent undervote in some elections, and now these machines have essentially ended that problem.

And so it is way more—the glass is way more than half full.

Mr. SELKER. I want to corroborate that and say we now have several States that have less than half a percent residual. We believed in 2001 the lowest you could go because of protest votes was 1 percent. It is just remarkable.

The fact is that people are comfortable with the voting systems that they use. That is what exit polls tell you, and what we—I remember talking to this 80–year-old in Nevada, and I asked her, how did you find that experience? She had had the hardest experience all day. She rolled out of her mouth, "Well, those punch cards

were terrible. The leverage machines, I could never find anything. The optical scans I couldn't read. This is so fabulous." and I just couldn't believe she put it all in one sentence what she felt about that.

The big print people like high-contrast things. You know, if you do one raise per screen, you can get people to have a lot less errors. But I think that we are in a fantastic position now to improve elections with the technologies that we are now starting to get better.

Mr. PIERCE. My experience in Cook County in Chicago are people with disabilities are very satisfied and pleased that more options are available and more flexibility has happened. There is limitations with the machines that are available for this paper system, and those have access issues of their own.

Mrs. DAVIS. I was going to follow up.

In the disability community, which individuals have the greatest difficulty voting, and is there a way to kind of focus in on that particularly?

Mr. PIERCE. It is generally blind persons and those with some kind of motor impairments who have difficulty holding a pencil or pen in their hand and handling paper and manipulating paper would be the—is my observation.

Mr. SELKER. Fifteen percent of Americans have reading disabilities. Those people, drawing those eyes across the ballot, whatever the ballot is, is a problem. If you take a look at the ballots in Massachusetts, we only have the last names of the candidates on there, and you have to go across the ballots to get to the bubble. I think there are a lot of people with problems, and I think the sightless are among them, but not at all the largest number.

Mrs. DAVIS. Thank you.

I had an opportunity to go review a number of those machines today. I just want to thank the Chairwoman for making those accessible to us so that we would have that opportunity. And one of them, in particular, I did find that was supposed to help the disability, I was having a little difficulty with it.

So I think we all have to try them out and try and understand where some of the problems are. I know the problem I was having was—they were talking about having that fixed. But it was interesting to me that I was having a little difficulty with that hand motor coordination, I think.

Thank you.

Ms. LOFGREN. And that is from someone who votes a lot, all day every day.

I would like to thank this panel for taking the time to be with us today personally, and especially for your written testimony which is going to be key to us as we move forward looking at this issue. We are really honored by your presence. Thank you so much.

The CHAIRWOMAN. Madam Chair, may I just say, I am very impressed with this panel, but more so the secretary of state of Mississippi. And I am going to—hopefully we get back with you at a later date to really look at what you have because it seems like a great success story.

Mr. CLARK. Thank you, Madam Chair. You are very kind.

Ms. LOFGREN. Thank you all very much.

Ms. LOFGREN. Let me welcome panel number two.

This is a great opportunity for the committee to gain insight into the technical issues of these machines, and I think, as has been mentioned, there is a great anxiety among many people in the country about whether or not their vote is being counted accurately, not accurately.

People—since I am from the Silicon Valley, I know you will all take this in the right way. This is our Geek Squad here. We value you are here to talk a little bit about the technology and to give us the benefit of your expertise and your points of view.

So I wonder if we could just start with Mr. Zimmerman here from the Electronic Frontier Foundation and move on to Dr. Williams.

STATEMENT OF MATT ZIMMERMAN, STAFF ATTORNEY, ELECTRONIC FRONTIER FOUNDATION; HUGH J. GALLAGHER, MANAGING DIRECTOR, ELECTION SYSTEM ACQUISITION AND MANAGEMENT SERVICES, INC.; BRIAN BEHLENDORF, FOUNDER AND CHIEF TECHNOLOGY OFFICER, COLLABNET; DAVID WAGNER, Ph.D., ASSOCIATE PROFESSOR, UNIVERSITY OF CALIFORNIA, BERKELEY; AND BRIT WILLIAMS, Ph.D., PROFESSOR OF COMPUTER SCIENCE AND INFORMATION SYSTEMS, KENNESAW STATE UNIVERSITY

STATEMENT OF MATT ZIMMERMAN

Mr. ZIMMERMAN. Thank you, Madam Chair.

Good afternoon. Thank you for the opportunity to speak with you today on this important topic. I am a staff attorney with the Electronic Frontier Foundation, a San Francisco-based nonprofit, member-supported civil liberty organization that challenges industry, government and the courts to protect rights in the emerging digital world.

This discussion is about many things, but at its heart is the real issue of how the current generation of voting systems has relegated, in a structural way, real transparency to a secondary value. Given the time, my aim here is to touch briefly on a number of experiences that we have encountered that I think highlights some of the problems that are being caused or exacerbated by closed election systems, problems that be can be alleviated to a large extent by a move towards an open- or closed-source regime.

First, election monitoring, as a general matter, suffers in its ability to uncover and act upon useful information. Despite many documented problems through many election-monitoring efforts, despite these documented problems which are often not documented by election officials themselves, incidents were not investigated or investigated in only a limited way by the very election officials and vendors whose decisions and actions were at issue.

Second, and more important from my standpoint, postelection litigation aimed at investigating such suspect machine performance and correcting problems that appear to have resulted in incorrect election outcomes have fared little better. For example, EFF currently serves as cocounsel in Fedder v. Gallagher, a suit questioning the administration of a 2006 congressional race in Sarasota. This is a different race than is right now before the House. Far from accommodating the legitimate concerns of the Sarasota voters,

the State, the county, and the vendors closed ranks here and continued to prevent the independent type of inquiry into the source code and other relevant materials that we think is necessary.

Over the past several years, I have had the distinct pleasure of working on this and related issues in an ever-growing community of very passionate people of all stripes who sometimes disagree and disagree very passionately about tactics. But a common thread that holds us all together is a shared belief that whatever the individual technological solution turns out to be, secrecy cannot continue to operate as a cornerstone of electronic administration. Voters want to be able to cast ballots and to have their ballots counted, but even more than that, they need to be convinced that the process is a fair and accurate one.

This perpetually increasing interest of the general public in the literal mechanics of the electoral process is, to borrow a computer programming term, a feature and not a bug. This is a good thing, not a bad thing. And I respectfully suggest that Congress should not be in the business of trying to dissuade the public from prioritizing transparency over a single component of the proprietary interest of vendors.

Thank you.

Ms. LOFGREN. Thank you very much.

[The statement of Mr. Zimmerman follows:]

Before the
U.S. House Committee on House Administration
Subcommittee on Elections

"Machines & Software"
March 15, 207

Statement of Matt Zimmerman
for
The Electronic Frontier Foundation

Good afternoon and thank you for the opportunity to speak with you today on this important topic. My name is Matt Zimmerman and I am a Staff Attorney with the Electronic Frontier Foundation, a non-profit, member-supported civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry, government, and the courts to support free expression, privacy, and openness in the emerging information society. Over the past three years, I have been responsible for EFF's e-voting reform efforts, work that has included promoting regulatory and legislative change, election monitoring, providing technical and legal resources to voters who encounter problems on election day, and, when necessary, litigation. It is my hope that my and EFF's experience in these matters will prove useful to the Subcommittee as it considers the wide range of issues and proposals before it.

It is axiomatic that the rights and interests of voters do not begin and end at the moment they cast their ballots. *See, e.g., Reynolds v. Sims*, 377 U.S. 533, 554 (1964) ("It has been repeatedly recognized that all qualified voters have a constitutionally protected right to vote, and to have their votes counted."). Voters have a profound interest in not only the physical act of voting but in the fair, secure, and accurate administration of the election process. In its most straightforward terms, the right to vote must include the right of voters to be able to understand and verify that the winner of an election is actually the candidate or proposition that received the most votes.

That right is at risk today due to seemingly unintended consequences of previous Congressional decisions. In the rush to abandon punchcard systems and other outdated equipment, whose flaws were all-too clear in the aftermath of the 2000 presidential election, Congress subsidized and state and local governments embraced and implemented new technologies in ways that critically hampered the ability of the public to monitor their elections. The central culprit of this elimination of transparency was the widespread deployment of direct recording electronic ("DRE") technology, which utilizes software and systems that are kept secret from not only the public but often from the very election officials who choose and run the machines on election day. The push for election officials to use DRE technology has created a crisis of confidence in our election systems that shows no sign of abating.

Today's discussion is about many things but at its heart is the very real issue of how poorly conceived systems have relegated real transparency to a secondary value in election administration. The question for this panel is whether or not transparency should be restored. One of the key proposals aimed at increasing transparency is to require that election systems contain open source or disclosed source code, rather than continuing with a closed model. While others on this panel can speak more completely on topics such as the security and viability of such systems, EFF is fully supportive of open and disclosed source voting solutions and believes that, while not completely solving the problems discussed today, they would serve as a major step forward.

My primary focus today is to briefly highlight some of the problems that are being caused or exacerbated by closed election systems. EFF has served, among other roles, as both election observers and as legal counsel for voters who felt compelled to challenge the use or results of apparently malfunctioning voting equipment. In both capacities, we and others have been severely hampered by the lack of transparency inherent in the current closed technological regime. For both of these purposes, the use of open or disclosed source voting technology as a component of a more open election process would immeasurably and demonstrably lead to a more confident electorate.

First, in the area of election monitoring, for the 2004 and 2006 general elections, EFF recruited and trained dozens of lawyers and law students to serve as voting technology experts for Election Protection, the nation's largest non-partisan voter protection coalition. In that capacity, EFF volunteers operated as technology liaisons, assisting voters and even election officials with technology-related problems that occurred in the field on election day. Volunteers with Election Protection and other independent monitoring efforts recorded hundreds of examples of machine irregularities that occurred across voting system platforms as well as across the country: votes jumping from one candidate to another, votes changing on summary screens, machines rebooting during the middle of voting, machines crashing and not returning to life at all. While the Election Protection program was enormously successful in documenting a slice of the election-day performance of voting machines, this analysis likely only amounts to the tip of a much larger iceberg.

And yet despite these documented problems – which were often not documented by election officials themselves – the incidents were frequently not investigated or investigated only by the very election officials and vendors whose decisions and actions were at issue. Moreover, the sort of thorough analysis necessary to comprehensively diagnose and fix problems, including a robust source code analysis in order to determine whether hidden problems in the system's programming could be at fault, was not on the table in those infrequent investigations. And of course since the election systems were fundamentally closed, neither the voters nor election advocates could conduct independent investigations of their own.

Second, post-election litigation aimed at investigating suspect machine performance and correcting problems that appear to have resulted in incorrect election outcomes fared little better. For example, EFF currently serves as co-counsel in *Fedder v. Gallagher*, a suit questioning the administration of the 2006 Congressional race brought by a group of bi-partisan voters in Sarasota County, Florida, a related yet separate and distinct case from the contest brought before the House of Representatives by Democratic challenger Christine Jennings. EFF and our co-counsel sought targeted machine-related discovery, including the source code of the voting machines, in response to widespread reports of problems along with a documented DRE undervote rate of nearly 15% that was recorded in Sarasota County – a rate approximately five times higher than expected by any of the experts in the case, amounting to approximately 14,000 excess undervotes in a race decided by less than 400. Far from accommodating the legitimate concerns of these Sarasota voters, the state, the county, and the vendors closed ranks to prevent any independent inquiry into not only the source code but other relevant materials such as operating instructions and other training of pollworkers who might have programmed or operated the voting machines. Their collective decision to deflect an independent inquiry into the voting machines and code was upheld by a single state court judge, a decision currently on appeal.

The right answer from a policy perspective is not only to allow independent access to election system source code and related components after a system demonstrates serious

problems, it is to make the source code and other critical materials available for independent expert review prior to the widespread implementation of voting technology. Had that been done in Sarasota and elsewhere across the country, independent experts would likely have been able to identify any serious deficiencies in the design and construction of the voting systems and helped prevent the loss of votes in the first place. The few independent examinations of voting systems that have thus far taken place – which have been severely limited in scope – have uniformly found problems of varying degrees of seriousness that could potentially impact the accuracy of the system's operation or leave the system vulnerable to attack. But even if pre-implementation review is not possible, source code and other critical materials should be made available after the implementation of voting systems, especially after problems have been reported during elections, to allow independent experts to work with vendors and election officials to help diagnose reported problems and to help present to the voting public a picture much closer to the truth.

Various objections will be levied against attempts to move towards an open or disclosed source voting technology regime, but whatever challenges that transition causes, I respectfully submit that they pale in comparison to the immeasurable good it will do to restore confidence in a system that first and foremost serves the interests of voters. Some claim that open source systems are fundamentally less secure, but computer science experts, including my co-panelist, can confirm that open source systems are fully capable of handling the important security requirements demanded of our election systems, as evidenced by the wide range of secure, commercially viable systems on the market today. Others claim that open source systems will result in the evisceration of intellectual property protections, but this too is untrue. While the use of absolute trade secret protection in this context is inconsistent with election transparency, vendors are still free to protect their products through copyright and patent protections that should be more than adequate to protect any genuine innovation.

Transparency is not a panacea, and mandating the disclosure of voting system source code does not resolve all of the shortcomings in our nation's election system. These steps will, however, provide a legitimate, defensible basis for the return of voter confidence that is sorely lacking in the current generation of closed election technologies. It is only when voters have a persistent, ongoing, independent basis to believe that their elections were conducted fairly that they will begin to fully trust in the integrity of their electoral process once again.

Again, thank you for the opportunity to appear before the Subcommittee to address these important issues. We appreciate being asked to be here and look forward to working with you and your staff as you examine these issues further.

Ms. LOFGREN. We are lucky to have Dr. Williams, a professor of computer science from Kennesaw State University.

STATEMENT OF BRIT WILLIAMS

Mr. WILLIAMS. Thank you. I want to begin by thanking you, Madam Chairwoman, for giving me this opportunity to appear before you. I have worked in this area of evaluating voting systems for over 20 years. I appreciate the opportunity to share this experience with you.

If you look at the definition of "open source," you will find that it talks about making the source code available to the public and allowing users to alter them. Nowhere in the definition or the literature does it mention that open source is a mechanism for testing source scope or establishing the validity of source scope. And there seems to be a general conception that source scope is unavailable to be reviewed, and this is not the case.

In my experience over the last 20 years, everyone I am aware of who has any need to evaluate or any legitimate need to evaluate source code has had access to it.

I have been evaluating voting systems for the State of Georgia since 1986, and I have had in my possession the source code of every voting system that has been used in the State of Georgia during that period. So the source code is available. It is not available to the general public. And I have got some serious concerns over whether the source code should be available to the general public, because the general public includes everything from teenage hackers to foreign terrorists, and I don't think this is what the committee has in mind.

So, in my opinion, open source code is not a good idea. But should the source code be available for evaluation? Absolutely, but under very carefully controlled conditions that, number one, protect the proprietary nature of the source code itself, but, more important, protect the security of the United States and its elections.

So right now, for example, source code is evaluated at the Federal level, and it is archived there. It is evaluated at the State level, and it is archived there. So it is available.

And what I would like to end with is a recommendation for evaluating source code, and I am using a model that was just used in the State of Florida to evaluate the source code that I believe you were involved in that. And I will leave him to talk about that.

But number one, I think the evaluation of a source code should be under the auspices of a State election organization; that the individuals that would be evaluating that source code would be selected by that State; and that the election official would then apply to the EAC for a license, if you please, to obtain that source code. I believe that the individuals who would participate in that should be subject to background checks by the Office of Homeland Security, and I believe that they should be required to sign a nondisclosure agreement where they agree to protect the proprietary nature of the vendor software.

And if I can have about another 10 seconds.

The final thing I believe is that there should be severe penalties for disclosing that software to any unauthorized person. And I think that should be spelled out in the code, because we have an

anecdotal evidence that our patent laws and our current laws on protecting proprietary software are not adequate to protecting voting system software.

Ms. LOFGREN. Thank you, Dr. Williams.

[The statement of Mr. Williams follows:]

Testimony before the
Committee on House Administration
Election Subcommittee Hearing on Election Reform
March 15, 2007

Britain J. Williams, Ph.D., Professor Emeritus
Kennesaw State University

Introduction

I would like to begin by thanking the Committee for the opportunity to appear before you. I have worked in the arena of computer based voting systems for over 20 years and appreciate this opportunity to share with you my experience and opinions on this important matter of open source software for voting systems. I will begin with some background information and then conclude with some specific recommendations.

Background

The following definition and description of open source software is intended to give the Committee a sense of what the various panel members intend when they take the position that voting system software should be *open source.* The two key points in the following are that under open source our voting system software would be "made available to the general public with either relaxed or non-existent intellectual property restrictions" and that this "allows the users (i.e. the general public) to create user-generated software."

The examples that are listed are mostly very specialized applications that are not in use by the 'general public.' For example, OpenOffice.org[1] is designed to compete with Microsoft Office. Although this product is free, I would be surprised to learn that a single member of this Committee has replaced their Microsoft Office suite with OpenOffice.org.

> **Definition:** *Open source* describes the principles and methodologies to promote open access to the **production** and **design** process for various goods, products,

[1] http://en.Wikepedia.org/wiki/OpenOffice.org

Testing and Certification of Voting Systems

The primary reason that is given for requiring voting system software to be open source is that open source would allow the public to verify the accuracy of the voting system software and detect any fraudulent code that may be present in the voting system software. In other words, open source would allow an extensive and through testing of the voting system source code.

Yet nowhere in the definition of open source is testing even mentioned. The definition of open source clearly states that the purpose is to allow users to modify the software to suit their own individual needs. Clearly, this is not the intent of this Committee.

Voting systems and their associated software currently undergo extensive tests and all of these tests are open to the public. Specifically, voting systems are tested at four different levels:

Federal
State
Local Acceptance
Local Logic and Accuracy

The following sections give a brief description of the tests performed at each level.

Federal Level Testing: From the mid 1990's until recently, voting systems were tested for compliance with the voting systems standards developed by the Federal Election Commission. These tests were under the direction of the National Association of State Election Directors.

As required by the HAVA, the Election Assistance Commission has developed Voluntary Voting Systems Guidelines (VVSG) and has put in place a process to ensure that voting systems comply with these Guidelines. Under EAC direction, Voting System Test Laboratories (VSTL) examine the voting systems for compliance with the Guidelines. To become a VSTL, a laboratory must first be certified by NIST and then be approved by the EAC.

resources and technical conclusions or advice. The term is most commonly applied to the source code of software that is made available to the general public with either relaxed or non-existent intellectual property restrictions. This allows users to create user-generated software content through either incremental individual effort, or collaboration.

- Open source software — software whose source code is published and made available to the public, enabling anyone to copy, modify and redistribute the source code without paying royalties or fees. Open source code evolves through community cooperation. These communities are composed of individual programmers as well as very large companies. Examples of open-source software products are:
    - Linux kernel - operating system kernel based on Unix
    - Eclipse - An IDE primarily for doing Java development, but has enough plug-ins to make it a software that can do virtually anything from programming in multiple technologies to creating Word documents and checking e-mail
    - Apache - HTTP web server
    - Tomcat web server - Java web/servlet-container
    - Blender - 3D graphics application
    - Moodle - course management system
    - Mozilla Firefox - web browser
    - Mozilla Thunderbird - e-mail client
    - OpenOffice.org - office suite
    - OpenSolaris - Unix Operating System from Sun Microsystems
    - Project.net - Commercial Open Source Project Management
    - Mediawiki - wiki server software, the software that runs Wikipedia
    - Aras Innovator - open source business process management enterprise software
    - Drupal - content management system
    - Joomla! - content management system
    - GNU Compiler Collection - Programming language compiler for C, C++, Java and other languages.
    - phpBB - open source bulletin board system
    - Nvu - open source WYSIWYG HTML editor (webpage/website builder)
    - Audacity - open source audio recording software
    - StCAD - open source 3D Framework for Smalltalk
    - Adempiere - open source ERP/CRM
    - FileZilla - open source FTP-Client [2]

[2] http://en.wikipedia.org/wiki/Open_Source

Based on the results of the VSTL examinations and any other information at their disposal, the EAC will certify the voting system as being compliant with the VVSG.

One of the tests performed by the VSTL is an examination of the voting system source code.

After EAC certification has been granted, the VSTL delivers the source code and the object code along with their digital signatures to a trusted archive designated by the EAC.

State Level Testing: After a voting system is certified by the EAC, each state that wishes to consider using the voting system conducts a state level test of the system. Historically, these state level tests have been little more than a review of the voting system for compliance with state law; however, most states have now responded to the increasing concern for voting system security by implementing state level tests that approach the rigor of the EAC tests.

Many states require the vendor to submit source code to the state. The state conducts a review of the source code and then archives the source code for future reference as needed.

Local Level Acceptance Testing: Most states will not allow a local jurisdiction to purchase a voting system until that system has received EAC Certification and State Certification. Upon delivery, the local jurisdiction conducts tests, called acceptance tests, that test the system for compliance with the conditions of the procurement and to verify that the system delivered is identical to the system that underwent EAC and State Certification.

Local Logic and Accuracy Testing: Prior to each election, the local jurisdiction conducts tests called Logic and Accuracy Tests (L & A Tests). These tests are a simulated test of all of the ballot styles and the entire set of voting system devices that are to be used in the upcoming election.

The voting system configuration for each precinct is set up and the ballot styles for that precinct loaded on the devices. Then ballots are cast on the system in accordance with a known pattern of votes. The precinct is then closed and the results recorded on the voting system are compared to the

results of the known pattern of voting. The local election officials must account for any descripancies.

These L & A tests are public tests that must be advertised in the local legal organ prior to the tests.

Organizational Use of Open Source Code

Every agency in government and every major business entity have software that is considered mission critical. I am not aware of a single organization that makes their mission critical software available to the general public. The reason is simply that open source software is vulnerable to attack from everyone from teen age hackers to foreign terrorists.

Voting system source code is mission critical to successful elections. Placing this source code in the hands of hackers and terrorists clearly creates the potential for harm to the integrity of elections. In addition, substantial harm can be done to a voting system by well-meaning members of the public. On the other hand, there are advantages to be gained from making this source code available to responsible reviewers.

It is recommended that the EAC be granted the authority to make voting system source code available to responsible individuals. Persons wishing to review voting system source code be should be required to make application to the EAC; providing their credentials for reviewing the software, their 'need to know', and the specific voting system software they wish to review. A recipient of voting system software should be required to sign a nondisclosure agreement and to return or destroy the software when their review is completed. Source code should only be provided to individuals, not organizations.

A Specific Recommendation

The following gives a recommended outline for allowing access to voting system source code. This recommendation is based on the belief that voting system source code should only be issued to individuals (not organizations) that are working under the direction a state or local election official. It also contains a feature that will allow the identification of any source code that is leaked to any unauthorized individual or organization. Finally, it is strongly recommended that there be specific, well defined penalties for violating the

confidentiality of voting system source code. It has been previously demonstrated that US Patent Laws and laws designed to protect proprietary information are not sufficient to protect voting system source code.

1. The cognizant election official must file with the EAC an application with the EAC requesting that a specific individual or group of individuals be allowed access to the source code for a specific voting system. This application must clearly state the reason for the request.
2. Each individual named in the application must then provide the EAC with the following information:
    - The reason the individual wishes access to the source code.
    - The qualifications of the individual to evaluate source code.
    - The schedule that the individual intends to adhere to while reviewing the source code.
3. The individual must sign a non-disclosure statement agreeing that (s)he will not disclose the source code to anyone that has not been approved by the EAC. The agreement must also specify that the individual cannot release any report or press release based on the review of the source code until the report or press release has been approved by the EAC. This agreement should clearly state the penalty for disclosing the source code to any unauthorized individual.
4. Once the EAC approves the application, the individual must undergo background checks by the Office of Homeland Security.
5. When steps 1, 2, 3, and 4 have been successfully completed the EAC will furnish the individual with a digitally signed copy of the source code. This digital signature must be unique to the point that it cannot be altered or duplicated.
6. When the schedule in step two expires the individual must either return the digitally signed source code to the EAC or apply for an extension.

Thank you

Again, I wish to thank the Committee for the opportunity to address these important issues. I sincerely hope that I have made at least a small contribution to the work of this committee.

In closing, I would like to state that the opinions presented in this paper are entirely my own. They do not represent the opinions of Kennesaw State University or the Office of the Georgia Secretary of State.

Respectfully submitted:

Britain J. Williams, Ph.D.
Professor Emeritus of Computer Science and Information Systems
Kennesaw State University

Brit Williams is Professor Emeritus of Computer Science and Information Systems at Kennesaw State University. He has worked in the field of computing since 1957. He has directed large computer centers and computer networks in industry, government, and academia. One of his primary research interests since 1986 has been computer-based voting systems. He was a consultant to the FEC during the development of the 1990 Voting System Standards and the 2002 Voting System Standards. He was a member of the NASED Voting Systems Board and Chair of the NASED Voting Systems Board Technical Committee from their inception until 2007. He represents NASED on the Technical Guidelines Development Committee created by the Help America Vote Act. Dr. Williams has been conducting certification evaluations of computer-based voting systems for the State of Georgia since 1986. He also has assisted the states of Pennsylvania, Maryland and Virginia with certification evaluations of computer-based voting systems.

Ms. LOFGREN. We also have Dr. David Wagner, who is a professor of computer science at California, Berkeley.

STATEMENT OF DAVID WAGNER

Mr. WAGNER. Thank you for the opportunity to testify today.

My name is David Wagner. I am an associate professor of computer science at U.C. Berkeley, and I work in computer security and electronic voting.

E-voting was introduced for laudable reasons; however, in addressing one problem, we have created several new ones. First of all, e-voting brings risk to election security. Over the past 4 years, independent researchers have discovered security vulnerabilities in voting machines used throughout the country. I will point out that our State and Federal certification processes designed to evaluate these voting systems failed to discover those vulnerabilities.

Would disclosing voting systems source codes help with the security risks? Yes, potentially, but with some very important caveats. Access to source code has improved security in other areas of computing, and I expect it could have the same effect here, too. That said, source code analysis does have important limitations. Source code analysis cannot—source code disclosure cannot solve the security problem. It cannot demonstrate that our voting machines are trustworthy.

When it comes to security, another path is to reduce our reliance upon software by moving to software-independent voting systems. For instance, adopting voter-verified paper records and routine audits of those records would be one way to achieve this. In my opinion, software independence would make source code disclosure less urgent from a security point of view.

A second problem is that the spread of voting machines has degraded the transparency of our elections. The secrecy surrounding the software makes it difficult for the public to observe and exercise meaningful oversight over the administration of our elections.

Let me give you an analogy. How would you feel if your taxes were computed for you each year by the IRS using a secret formula that you weren't allowed to see? I suspect many people would probably be pretty concerned about that, just as they are concerned by the fact that their votes are counted using secret codes.

Would source code help improve transparency? It sure would. Source code disclosure would help restore some of the transparency that was lost when we moved to electronic voting. For instance, disclosure would eliminate the vendors' information advantage over their customers and over the public. Today vendors make claims about their machines, and members of the public can't get access to the information they need to independently evaluate those claims. Source disclosure would enable candidates, political parties and interested members of the public to commission independent analysis of the machines and get a second opinion, something they cannot do today.

If we accept that source code disclosure is a good goal in the long run, there are, however, some difficult challenges about how to get there. Unfortunately, today's voting machines are not designed for disclosure, and that creates several challenges. One of those challenges is that, based on my experience reviewing source code from

two of the four major vendors, it is my prediction that immediate disclosure of source code could easily lead to discovery of serious problems in all of the vendors' machines, and that would overwhelm the ability of the vendors and the election officials to respond in a single election cycle.

So given these challenges, it might make sense to phase disclosure in over time. And in my written testimony, I have described several ways one might manage the transition by gradually increasing the scope of disclosure over several years.

Ms. LOFGREN. Thank you very much.

[The statement of Mr. Wagner follows:]

WRITTEN TESTIMONY OF DAVID WAGNER, PH.D.
COMPUTER SCIENCE DIVISION
UNIVERSITY OF CALIFORNIA, BERKELEY
BEFORE THE COMMITTEE ON HOUSE ADMINISTRATION, ELECTIONS SUBCOMMITTEE
U.S. HOUSE OF REPRESENTATIVES
MARCH 15, 2007

Chairwoman Millender-McDonald, Ranking Member Ehlers, committee members, thank you for the opportunity to testify today. My name is David Wagner. I am an associate professor of computer science at U.C. Berkeley. My area of expertise is in computer security and the security of electronic voting. I have an A.B. (1995, Mathematics) from Princeton University and a Ph.D. (2000, Computer Science) from U.C. Berkeley. I have published two books and over 90 peer-reviewed scientific papers. In past work, I have analyzed the security of cellphones, web browsers, wireless networks, and other kinds of widely used information technology. I am a member of the ACCURATE center, a multi-institution, interdisciplinary academic research project funded by the National Science Foundation[1] to conduct novel scientific research on improving election technology. I am a member of the California Secretary of State's Voting Systems Technology Assessment Advisory Board and of the Election Assistance Commission's Technical Guidelines Development Committee (TGDC)[2]. I have served as a poll worker in my county, and I served as a technical advisor to my county's equipment selection committee.

In my testimony today, I will address source code disclosure, the problems it is intended to solve, and its benefits and risks. There are peculiarities in the voting system market and regulatory process that complicate the transition to the disclosure of the voting system source code. While these peculiarities require that such a transition be carefully considered and managed, it is a transition that I view as important for sound elections, for three reasons: (1) security and reliability; (2) public confidence and transparency; and (3) oversight and accountability.

A primer on source code and its the role in elections

What is source code? Source code is the human-readable representation of the instructions that control the operation of a computer. Computers are composed of hardware (the physical devices themselves) and software (which controls the operation of the hardware). The software instructs the computer how to operate; without software, the computer is useless. Source code is the human-readable form in which software is written by computer programmers. Source code is usually written in a programming language that is arcane and incomprehensible to non-specialists but, to a computer programmer, the source code is the master blueprint that reveals and determines how the machine will behave.

Source code could be compared to a recipe: just as a cook follows the instructions in a recipe step-by-step, so a computer executes the sequence of instructions found in the software source code. This is a reasonable analogy, but it is also imperfect. While a good cook will use her discretion and common sense in following a recipe, a computer follows the instructions in the source code in a mechanical and unfailingly literal way; thus, while errors in a recipe might be noticed and

[1]This work was supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

[2]I do not speak for UC Berkeley, ACCURATE, the California Secretary of State, the EAC, the TGDC, or any other organization. Affiliations are provided for identification purposes only.

corrected by the cook, errors in source code can be disastrous, because the code is executed by the computer exactly as written, whether that was what the programmer intended or not. Also, computer software is vastly more complex than most recipes: while a typical recipe may contain perhaps a dozen steps and fits onto a single 3x5" index card, computer source code often contains hundreds of thousands of steps which, if printed, would fill up thousands of single-spaced 8.5x11" sheets of paper.

What does source code have to do with elections? Over the past several decades, as we have automated more and more of elections operations, elections have become increasingly reliant upon computing technology. For instance, touchscreen voting machines use computers to capture votes; paper ballots are scanned using computer-driven scanning machines; and computers tabulate and tally the votes to determine the winner. This makes the software that controls these machines of critical importance to our elections.

The source code in voting machines is in some ways analogous to the procedures provided to election workers. Procedures are instructions that are provided to people; for instance, the procedures provided to poll workers list a sequence of steps that poll workers should follow to open the polls on election morning. Source code contains instructions, not for people, but for the computers running the election; for instance, the source code for a voting machine determines the steps the machine will take when the polls are opened on election morning.

Who writes election-related software? Today, counties and states buy voting equipment from commercial vendors. These voting system vendors write most of the software in their machines. However, voting system vendors also incorporate software from third-party software vendors into their products. For instance, a voting system vendor like Diebold might license software from Microsoft for use in their touchscreen voting machine. The voting vendor might or might not receive source code to the third-party software; if they do, they normally would not have permission to redistribute this third-party source code to others. Third-party software is sometimes called COTS (commercial off-the-shelf) software, which we'll cover later.

Who sees election-related source code? Today, most voting system vendors treat any source code they write as confidential and proprietary. The vendors tightly control access to this source code. Election officials use the equipment, but they are normally not given access to its source code. Candidates, political parties, technical experts, and interested citizens are normally not given access to voting system source code, either.

Federal voting standards require voting system vendors to share their source code with a testing laboratory selected by the vendor, and the testing labs are supposed to check that the system complies with the federal standards. However, the testing labs have come under growing criticism for missing security and reliability problems in deployed voting systems, and many experts have expressed concerns about the ability of the testing labs to ensure that voting systems are fit for use[1] [2].

Most states do not receive or require access to voting source code. However, there are some exceptions[3]. Five states appear to require source code for certified voting systems prior to their use (FL, NY, TX, UT) or have the authority to demand source code at their discretion (CA). Two states go farther and require that the vendor provide source code to representatives of the major parties upon request (NC, MN). In California, three of the four major vendors have pledged that if California passes a law requiring source code disclosure to the public, they would abide by those provisions.

What is COTS? The federal standards provide a special exemption for COTS (commercial off-the-shelf) software. The standards define COTS software as third-party software that is commercially

readily available. COTS source code is exempted from inspection or analysis by the testing labs. This exemption makes it possible for voting system vendors to use software developed by third-party vendors even though they may not be able to provide that source code to the testing labs. In practice, most of the third-party software found in today's voting equipment qualifies as COTS. For this reason, people sometimes loosely use the term COTS to refer to any software from third-party vendors, even though strictly speaking these two concepts are not identical.

What is firmware? In much of the software industry, "firmware" usually refers to software that is embedded in a hardware device by the manufacturer and that cannot be modified. However, in the voting industry, the term has expanded to encompass any software that executes on any elections-related equipment. Therefore, when I refer to "software" in my testimony, it should be understood to include what the voting industry calls "firmware."

What can analysis of election-related source code reveal? Computer programmers are trained in reading and analyzing source code. A programmer can read source code and use this to tell how the machine will work on election day. Source code analysis can find many kinds of defects or problems with the design or implementation of the machine. It can help assess the reliability or accuracy or security of a voting machine. Source code analysis can also help to improve testing: tests devised with the assistance of source code analysis are usually more effective than tests devised without this access.

Many kinds of defects and problems with voting machines can only be found with access to the source code. Security, in particular, is difficult to evaluate without access to source code. These kinds of problems often cannot be detected through testing alone. In general, source code analysis is one of the most effective methods we have for assessing the security, reliability, and accuracy of voting machines.

However, source code analysis nonetheless has significant limitations: it generally cannot guarantee that a voting machine is secure, reliable, accurate, fair, or fit for use in elections. This is due to two reasons. First, it is often difficult to be certain that the source code one is analyzing is the same as what will be executed by the voting machine on election day. Second, given the complexity of election-related software, it is generally not possible to be certain that you have found all the bugs in the software, and it is generally not possible to be certain that the software will work reliably and accurately on election day. This means that source code analysis can be used to show the presence of defects in voting software, but usually it cannot convincingly demonstrate the absence of defects. Source code analysis alone is unlikely to be able to demonstrate that voting machines are trustworthy.

Source code disclosure: pros and cons

Today, candidates, election officials, experts, and interested citizens do not have a right of access to voting system source code; vendors are allowed to keep this source code secret. Should vendors be required by law to disclose their source code more broadly? I will attempt to list the advantages and disadvantages I can see of mandating source code disclosure.

Source code disclosure could follow a number of models. The important variables are (1) who will have access to the source code and (2) what will they be allowed to do with it. I don't propose a specific model here, but parts of my discussion will assume that election jurisdictions and independent experts will have access to source code and will be able to use that access to read and analyze the code.

Arguments for source code disclosure:

- *Transparency:* Historically, one of the abiding principles of election administration has been that the best way to demonstrate that the election is honest is by inviting public scrutiny and being open and transparent about all aspects of the election. When any aspect of election administration is kept secret, it invites questions about whether the secrecy is intended to cover up problems or to stifle debate.

  The trend in elections is towards automation of more and more tasks that were previously performed manually. However, the spread of automation has unintentionally come with the unfortunate side-effect of degrading transparency[4] [5] [6]. When poll workers run elections or elections official count ballots, the public can observe that the actions are being done correctly and openly, and can spot any errors or problems. However, when those same operations are performed by machines, the secrecy surrounding those machines and their programming effectively prevents the public from meaningfully observing or engaging in oversight of the process. Disclosure of voting system source code to the public would help to restore the public's ability to observe and exercise public oversight over the equipment and its role in the administration of the election[7].

- *Informing public debate:* There has recently been considerable public debate about the trustworthiness of voting machines. Some have argued that current voting machines are severely flawed; others have disputed that characterization. However, because of the secrecy surrounding voting software, advocates on both sides of the debate have often been denied access to the information that would be needed to present evidence for their position. The result is that advocates are all too often forced to argue from first principles or based on their professional judgement, rather than from hard evidence.

  Source code disclosure would make it possible to have a more informed debate on the trustworthiness of today's e-voting machines. We could expect and insist that anyone who wants to argue that the voting software from one vendor is flawed should be able to point to where exactly in the source code the flaw may be found. We could expect and insist that anyone who wants to argue that the voting software is flawless should be able to show evidence that the source code is free of flaws. This would create the opportunity for a more informed and scientific debate regarding the trustworthiness of e-voting, and it might raise the level of the debate.

- *Better evaluation:* Source code disclosure would enable independent analysis of voting machine software. Given the importance and public visibility of this topic, I expect source code disclosure would lead some of the country's best independent technical experts to analyze the source code and publish their findings. There is reason to expect that such independent analyses would improve our understanding of the strengths and weaknesses of machines and remedy some of the shortcomings of the federal voting system certification process. This would provide voters and concerned citizens with information to help them assess the equipment they vote on. It would also help local and state election officials to make better procurement and certification decisions.

  The value of independent evaluation is probably most pronounced when it comes to security. Security flaws can sometimes be subtle and easy to miss, even for experts. For this reason, enabling more people, especially security experts, to review the software significantly increases the likelihood that security problems in the code will be found.

- *Accountability:* The testing labs have been criticized for doing a poor job of evaluating voting systems. There have been a series of documented failures of the testing labs to discover

serious security and reliability problems in the voting equipment they approved. In my own examinations of voting system source code at the request of state election officials, I found serious defects in the source code that should have been immediately apparent to anyone with expertise in security. One cannot help but wonder whether the testing labs have anyone qualified in security reviewing the source code.

These failures may be due to structural problems in the way that testing is performed. Because testing labs are paid and selected by the vendor who makes the equipment being tested, testing labs are surely aware that withholding approval too frequently might send vendors to competing testing labs with a reputation for more lenient treatment. Elsewhere in the software industry, a similar "race to the bottom" has been observed in labs that test compliance to international computer security standards[8]. Unfortunately, at present there are few checks and balances that can be used to hold testing labs accountable if they fail to serve the public interest. In the long run, source code disclosure might help to ensure that the process is effective by holding testing labs accountable in the court of public opinion if they approve systems with obvious defects in the source code.

- *Improving voting machines:* In the long term, source code disclosure could have the effect of improving the quality of voting system software. First, source code disclosure allows a large community to spot bugs and problems so they can be corrected before they cause problems in the field. Because it is often hard for people to spot problems in their own work, a fresh eyes can see things that people who are most familiar with the code can miss by providing a fresh perspective. Second, source code disclosure would give vendors a powerful incentive to make sure their code is of high quality, to avoid public embarassment.

- *Promoting competition:* Source code disclosure would eliminate one barrier to interoperability between equipment from different vendors, potentially enhancing competition between vendors and providing more options to local election officials. Today, election officials cannot mix and match equipment from multiple vendors within the same jurisdiction. The business model adopted by the major vendors is based upon locking in counties as a captive customer of a single vendor. If the county wants to upgrade or enhance their system, any components they buy must come from that vendor. Unfortunately, this reduces the choices available to local election officials, reduces competition, and makes it harder for new companies with innovative products to enter the voting system market. Vendors use the proprietary nature of their code as one tool to keep counties captive. Source code disclosure would allow new vendors to enter the markets and build equipment that interoperates with the major vendors' equipment. This could potentially break the sole-source relationship vendors currently have with the counties and provide more alternatives to local election officials. However, achieving the benefits of interoperability would likely require changes to how we certify voting systems to permit certification of mixed-vendor systems.

  Source code disclosure could also allow new companies to provide maintenance and support services for equipment built by the major vendors. This, too, would promote competition and provide election officials with more choices. In today's personal computer (PC) market, one vendor (e.g., Dell) provides the hardware and another (e.g., Microsoft) provides the software. This model has increased competition between vendors, lowering prices for PC users. It is possible that opening the voting market to new vendors could reduce prices for voting systems in the same way that it has for PCs.

Arguments against source code disclosure:

- *Disclosure isn't sufficient:* Source code disclosure alone cannot ensure that voting machines are trustworthy, because of the limitations of source code analysis mentioned earlier. For instance, analysis of disclosed source code cannot ensure that the equipment is free of security vulnerabilities or malicious logic designed to rig an election[9], and it cannot ensure that the voting machines will be fair and accurate.

  At present, the best tool we have for ensuring that votes are counted accurately is to use voter-verified paper records and perform routine manual audits of the paper records[10] [11]. Adoption of voter-verified paper records and routine audits would reduce our reliance on source code analysis to ferret out security and reliability problems in the software.

  The TGDC, a body which helps to set federal voting system standards, has recently endorsed a requirement that voting systems be *software-independent*[12]. A voting system is considered software-independent if an undetected change or error in the voting software cannot cause undetectable changes or errors in the outcome of the election[13]. For instance, voting systems with a voter-verified paper record are considered software-independent, because the voter-verified paper records can be used to audit or recount the election results. Software-independence reduces some of the urgency for source code disclosure, by reducing (but not eliminating) the impact that defects in the source code can have.

  In general, we can rate voting systems by the degree to which they rely on software:

  - Paperless e-voting systems are completely dependent on the correctness of their software.
  - Adding a VVPAT printer reduces the dependence on software.
  - Paper-based optical scan systems reduce this dependence even further, and hand-counted paper ballots eliminate dependence on software.

  Generally, the more the system depends on the correctness of its software, the greater the likelihood of reliability and security problems. Of course, software independence is just one among several considerations in the choice of a voting system.

- *Transition risks:* If source code disclosure is mandated with insufficient advance notice and the transition isn't managed properly, there is a risk that in the short term disclosure could create more problems than it solves. Based on my experience[14] [15] reviewing the source code of some voting software, it is my prediction that immediate disclosure of source code would likely lead to discovery of serious problems in all vendors' machines.

  It is not clear that vendors could respond and fix these problems within a single election cycle. Even if they could, the process of repairing all of these problems and approving and deploying the patches could place a heavy burden on existing certification processes and on election officials. In the election world, the time between identification of a flaw and the availability of a patch for it is often painfully long. For instance, it has been over a year since two serious security vulnerabilities were identified in one voting system by Finnish researcher Harri Hursti[16] [17], but still no solution is available to election officials, despite the fact that one of these vulnerabilities was labelled by some security experts as the worst vulnerability they have ever seen in a voting system[18]. As another example, one system contains a security vulnerability that was reported privately to the vendor in 1997[19], disclosed publicly in 2003[20], confirmed to be still present in a 2004 report[21], was still present when I examined the system in 2006[22], and remains unresolved to this day[23]. Looking to the future, it is possible that immediate source code disclosure might lead to the discovery that every e-voting system in

widespread use has multiple problems that cannot be addressed through procedures and that cannot be repaired in time for the election. Depending upon the timing, all machines in the country could have to be re-designed, re-implemented, and re-certified in a single election cycle. In practical terms, this would be a disaster.

These risks can probably be mitigated if appropriate plans are put in place to manage the transition to source code disclosure smoothly and if disclosure requirements are phased in over time.

- *Giving aid to attackers:* One serious concern is that disclosing voting system source code might aid attackers to find and exploit vulnerabilities in voting systems. This is indeed a valid concern. Throughout the history of computer security, experts have struggled with this risk.

  At the same time, this concern must be tempered with a recognition that this is a complex issue. If the voting system contains vulnerabilities, lack of source code will only slow down, but not stop, a dedicated attacker. For that reason, security experts usually recommend that it is far safer to avoid vulnerabilities in the first place, and source code disclosure is one effective way to advance that interest.

  In computer security, it is widely accepted that well-designed systems should be constructed so that disclosing the source code does not endanger security. Kerkhoff's principle, which dates back to the 19th century, states that systems should be designed so that their security does not rely upon the secrecy of their design or implementation[24]. The reason is simple: if the leak of information about how the system works can compromise its security, then the system is fragile[25]. Practical experience shows that these secrets often leak—for instance, one vendor's source code was leaked onto the Internet in 2003—and even in the absence of leaks, a sufficiently dedicated adversary can get access to the same information through reverse engineering. Generally speaking, if the system can be hacked by an adversary with access to the source code, it can also be hacked by an adversary without that kind of access, so the presence of such a vulnerability is very troubling. For these reasons, the consensus in the computer security community is that systems should be designed to ensure that revealing the source code does not endanger system security.

  If we had confidence that existing voting systems were well-designed, we could disclose their source code without fear of helping attackers. Unfortunately, the concern is that existing systems are so poorly designed that source code disclosure could in the short run help attackers. In the long run, my experience is that disclosure helps to raise awareness of the problems among the users of the software, and thereby drives better security practices and forces systems to be better designed. However, this takes time. Therefore, my expectation is that in the long run source code disclosure would improve voting system security more than it hurts, but the transition must be managed carefully.

  One must be careful to avoid drawing the wrong conclusion. Some vendors and election officials have suggested that the secret, proprietary nature of voting system code is a key security measure, because giving people the source code would give them directions on how to hack it. Such statements reflect a disturbing lack of familiarity with computer security. I am not aware of any computer security expert who suggests that we should rely upon the secrecy of the source code as a key part of our strategy for securing our elections[26]; this would violate basic principles of secure design[27].

Open source vs. disclosed source. Some advocates have argued that election-related software should be developed through "open source" processes, where any interested party can contribute code to the elections software. "Open source" is a term of art in the computing industry. Open source software is software that is released under relaxed licensing terms. Recipients typically receive the right to modify the software for their own purposes and to re-distribute their modifications freely. This allows users to collaborate to improve the software on their own, without relying upon the original developer of the software. Open source software is often provided to users at no cost, and the software almost always comes with source code. Open source software is often, but not always, written by interested volunteers through a non-corporate, community-driven development process.

It is important to note that open source software is not the same as disclosed source software. Vendors can continue to use traditional software development processes and subsequently disclose the resulting source code, without any need to adopt any of the other distinguishing features of open source software. Source code disclosure policies, licensing terms, and software development processes are three separate matters, and while open source software takes a particular stance on all three topics, it is source code disclosure that matters most to elections.

While "open source" development processes do have advantages, I believe that mandating "open source" development would be inappropriate at this time. In comparison, source code disclosure is a much less radical step. In this model, vendors would continue to write and develop software themselves and would control the contents of the software, but they would be required to disclose the source code to certain parties.

The impact of disclosed source on intellectual property. Source code disclosure would not prevent vendors from competing on the merits of their source code and protecting their legitimate innovations. Source code disclosure would implicate several forms of intellectual property protection, but I wish to focus on issues involving copyright and trade secret protection. My understanding is that source code may be protected simultaneously under copyright law and trade secret law.

Before addressing these issues, however, I'll address an initial question that the previous sections of my testimony might provoke: If source code disclosure, or publication of source code under an open source license, offers long-term advantages to voting system vendors as well as the election system as a whole, why haven't vendors already moved in that direction on their own? The answer, I think, is that if one vendor discloses their source code and another does not, the disclosed-source vendor has no way of knowing whether their rights are being violated by the closed-source vendor. Therefore, the marketplace discourages vendors from going to a disclosed source model on a voluntary basis.

Vendors would retain copyright protection in their source code, even if the code were openly published. This is not unlike publishing a book. When an author publishes a book, it is protected under copyright law, and the author can assert the rights granted by copyright law to prevent others from making unauthorized copies. This allows the author to sell copies while providing recourse against people who would make wholesale copies of the book without permission. Just as importantly, recipients can read the book and quote excerpts for criticism or other kinds of fair use. In a similar vein, recipients of voting system source code under could read and analyze the code, but copyright law would prohibit them from making wholesale copies of the source code. As a result, vendors' interests in preventing competitors from free-riding on their efforts would be protected.

Some source code disclosure models might well threaten a vendor's current ability to require counties to use equipment from that vendor, and that vendor only; but the increased competition, innovation, and flexibility would serve important public interests in the election system.

Source code disclosure does raise difficult questions about trade secret protection. Unrestricted

disclosure would likely destroy any trade secret protection in the source code, but some of the more controlled forms of disclosure (as I discuss later) would preserve the possibility of protecting trade secrets. Whether trade secret protection is appropriate for source code in certified voting systems is a question that I'm not qualified to answer on my own, but it is one that I hope this Committee will examine very carefully. Specifically, the public interest in transparency and accountability warrant close attention[28].

Source code disclosure also eliminates the vendors' "information advantage" over their customers and the public. At present, vendors can make claims about their software (e.g., that it is perfectly secure) without being contradicted. Source code disclosure would force vendors to be more circumspect about their claims—which may reduce the vendors' flexibility, but seems to be in the public interest.

Requiring source code disclosure of all vendors sets a level playing field. To the extent that source code disclosure has costs for vendors, vendors can set their prices to reflect the costs of disclosure.

Policy options

There is a broad spectrum of possible policy options that are available to address these issues.

Do nothing (status quo). One possibility is to make no changes to the status quo regarding source code disclosure and continue to permit vendors to treat their source code as secret and proprietary. The risk of doing nothing is that the lack of transparency may contribute to further loss of confidence in e-voting[29].

Mandate disclosure to the public. Another possibility is to require vendors to disclose the full source code for all the software in their voting equipment to any interested member of the public. This could be accomplished, for instance, by requiring vendors to disclose source code to the EAC as a condition of certification and requiring the EAC to publish it or provide it to members of the public upon request. There should be no possibility for vendors to protest; disclosure would be mandatory.

Intermediate steps. There are many small steps one could take that would incrementally move us towards increased disclosure without going all the way to full public disclosure all at once.

- *Mandate disclosure to the federal and state election officials.* The smallest step would be to require vendors to disclose source code to federal and state election officials. This would permit election officials, at their discretion, to commission independent technical experts to analyze the source code. One shortcoming of this approach is that election officials generally do not have the necessary technical expertise in-house; hiring paid consultants to perform the work is expensive; and some election officials might be reluctant to seek analyses that might reveal embarassing flaws in systems that they have approved and that are in widespread use.

  This step would likely have little effect on the status quo. The EAC already has the authority to demand that vendors disclose the source code to them as a condition of submission for certification, but has declined to exercise that authority[30].

- *Mandate disclosure to candidates.* The next step would be to require source code to be disclosed to all candidates and their representatives, such as any technical experts that they designate. Vendors would not be permitted to protest or prevent such disclosure. To prevent further re-distribution of the source code, the candidates' designated experts could be required to sign agreements not to further disclose the source code to third parties. However, it

is critical that these non-disclosure agreements be written to allow the experts to publicly discuss their findings and provide evidence to support their conclusions. The agreements must also be written to preserve the independence of the candidates' experts; vendors and officials must not be allowed to interfere with, limit, or pressure the candidates' experts. Non-disclosure agreements must not be used as a way to silence dissent or place barriers to meaningful review of the source code.

- *Mandate disclosure to local election officials.* Another option would be to require that source code be disclosed to local election officials and their designees. This would permit county officials, at their discretion, to commission independent technical analysis of the source code. This might help them to choose among multiple systems when buying new equipment, or to understand the strengths and weaknesses of their systems and craft appropriate procedural mitigations.

- *Mandate disclosure to qualified experts.* A final option would be to require that source code be disclosed to any qualified expert upon request, regardless of the expert's affiliation. Those experts might be required to sign non-disclosure agreements, as discussed earlier; access might be restricted to US citizens; and to avoid a conflict of interest, vendors might be forbidden from gaining access to their competitors' code. However, to ensure that such a requirement meets its goals, the definition of qualified expert must be crafted carefully to ensure that qualified people are not wrongly excluded. This is not a theoretical concern: one early attempt to draft such requirements[31] was flawed[32] [33] [34]. For instance, it might be reasonable to require either a graduate degree or at least five years of experience in computing.

Mandating disclosure to qualified experts would help improve voting machines, improve the evaluation process, hold vendors and testing labs accountable for their performance, and lead to more informed debate about voting systems. It would address concerns about public disclosure aiding attackers and help manage the transition.

Ultimately, though, this position is problematic in the long run, because it puts a small cadre of experts in a privileged position. This will be a constant source of dissatisfaction and friction for those who distrust whichever experts are permitted to study the code. While this does enhance security review, restricting disclosure to qualified experts fails to address the public interest in the transparency of voting software.

Phased introduction of disclosure requirements. One way to address the transition risks would be to gradually introduce these requirements over time. For instance, one possible timetable for increased source code disclosure might be as follows:

- One might require vendors to disclose source code to state and federal election officials immediately, and require election officials to promptly commission independent expert security analyses of the systems. Officials could require vendors to fix any security problems found in the code, to make the code safe for broader disclosure.

- Then, one might require source code disclosure to qualified experts, at their request, after enough time has passed to correct any problems found in the prior phase. Two years should suffice.

- Finally, one might require source code disclosure to the public at some future date specified in advance. Five years notice ought to be enough for vendors to prepare their code for public disclosure and to ensure that it can withstand scrutiny, so that we can be confident public disclosure will not assist attackers to attack elections.

It is important that the timetable be set and published now, so that vendors have enough time to ready their systems for public disclosure. Competitive pressures make it difficult for vendors to begin preparations without a concrete deadline.

If vendors are given sufficient advance notice, there is no reason they cannot ensure that their systems will be safe to disclose. A gradual introduction of source code disclosure requirements could minimize the transition risks while advancing the long-term goals of transparency and security.

Reducing dependence on software. Another policy option would be to reduce the severity of the source code secrecy problem by reducing our dependence upon software in elections. As discussed earlier, this could be achieved by mandating voter-verified paper records and routine audits. Adoption of paper ballots (whether optically scanned or manually counted) would further reduce the degree of dependence upon secret software and further reduce the need for source code disclosure. This direction would not address the public interest in transparency, but it would reduce or mitigate many of the other problems with secret code.

COTS software

The COTS challenge. COTS code poses a special challenge for mandatory disclosure of voting system source code. Many deployed voting systems contain COTS software written by third-party vendors, and the equipment manufacturer may not have access to the source code for that software or may not have permission to disclose it. Thus, any requirement to disclose the source code for all software in deployed systems could put some vendors in a serious quandary: they would either have to negotiate with the third-party software vendor for the rights to disclose that code; replace the undisclosable third-party software with code that they are free to disclose and seek certification for the new code; or withdraw their equipment from the market. Forcing the decertification of voting equipment that counties have already paid for would make life very difficult for local election officials who have an election to run. The impact of this is likely to vary from vendor to vendor, because some vendors rely more heavily on COTS code than others. While some vendors might not face such a quandary, forcing even one major vendor to recall their equipment on short notice would cause havoc for jurisdictions who use that vendor's equipment.

New systems would be unlikely to face this problem. There is no reason that voting equipment needs to contain undisclosable source code. Any competent engineer should be able to design voting equipment without resorting to third-party COTS code that cannot be disclosed, if source code disclosure is specified as a requirement at design time. Therefore, for new equipment, I do not see any barrier to full source code disclosure.

However, disclosing the source code of systems that were not designed to be publicly disclosed poses significant challenges. The problem is that existing equipment was not designed with source code disclosure in mind, and consequently some voting systems contain third-party COTS code that may not be easy to disclose or replace. This complicates the task of setting policy regarding source code disclosure.

Policy options. This problem with COTS code in legacy voting systems could be addressed in one of several ways.

- If vendors are given sufficient advance notice of the disclosure requirement, they should be able to ensure that their code is free of undisclosable COTS code. However, this "sunset" period for use of COTS code would delay imposition of the full disclosure requirement by several years.

- Another option is to exempt third-party COTS code from the source code disclosure requirement. Vendors would only be required to disclose source code for software they wrote themselves or that they otherwise have permission to disclose.

  However, this option is problematic, because COTS code can still cause problems. From an engineering point of view, COTS code is no safer than vendor-written code. COTS code can contain bugs and defects; it can contain malicious logic deliberately introduced to rig an election; and it can be manipulated or tampered with, just like vendor-written code. Therefore, any exemption for COTS code should probably be time-limited.

- Perhaps the least intrusive option is to introduce source code disclosure in a phased fashion. In the first phase, voting system vendors would be required to disclose as much source code as possible, including (at a minimum) all of the source code that they have written themselves. During the first phase, vendors would qualify for a limited-time exemption for COTS code, if they do not have the right to re-distribute its source code. In the second phase, after enough time has passed to allow vendors to replace all undisclosable COTS code or otherwise re-design their machines to ensure compliance, the COTS exemption would be eliminated and vendors would be required to disclose all election-related source code. To ensure the success of such a phased plan, it would be important to set a clear timetable in advance so that vendors can plan accordingly.

Notes

[1] B. Simons, "Electronic voting systems: the good, the bad, and the stupid", ACM Queue 2(7), Oct. 2004.

[2] D.W. Jones, "Misassessment of Security in Computer-Based Election Systems", Cryptobytes 7(2), Fall 2004, pp.9-13.

[3] P. Smith, "States with Escrow Provisions," March 12, 2007. `https://www.verifiedvotingfoundation.org/article.php?id=6439`

[4] D.W. Jones, "Voting System Transparency and Security: The need for standard models", written testimony before the EAC Technical Guidelines Development Committee, Sept. 20, 2004. `http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml`

[5] J. Hall, "Transparency and Access to Source Code in E-Voting," USENIX/ACCURATE Electronic Voting Technology (EVT'06) Workshop. `http://josephhall.org/papers/jhall_evt06.pdf`

[6] D.K. Mulligan, J.L. Hall, written testimony before the California Senate Elections, Reapportionment & Constitutional Amendments Committee, Feb. 8, 2006. `http://josephhall.org/nqb2/media/Mulligan_Hall_OSHRG_Statement.pdf`

[7] P.G. Neumann, Written testimony before the California Senate Elections Committee, Feb. 8, 2006. `http://www.csl.sri.com/neumann/calsen06.pdf`

[8] R.J. Anderson, *Security Engineering – A Guide to Building Dependable Distributed Systems,* Wiley, 2001, §23.3.

[9] J. Bannet, D.W. Price, A. Rudys, J. Singer, D.S. Wallach, "Hack-a-Vote: Demonstrating Security Issues with Electronic Voting Systems", IEEE Security & Privacy Magazine 2(1), Jan./Feb. 2004, pp.32-37.

[10] D.W. Jones, "Auditing Elections", Communications of the ACM 47(10), Oct. 2004, pp.46-50.

[11] A.D. Rubin, Written testimony before the Election Assistance Commission, June 30, 2005. `http://avirubin.com/vote/eac2.pdf`

[12] TGDC Resolution #06-06, "Software Independence of Voting Systems," Dec. 5, 2006.

[13] R.L. Rivest, J.P. Wack, "On the notion of 'software independence' in voting systems", `http://vote.nist.gov/SI-in-voting.pdf`.

[14] "Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, Feb. 14, 2006.

[15] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware," Feb. 23, 2007. `http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf`

[16] H. Hursti, Black Box Voting, "Critical Security Issues with Diebold Optical Scan", July 4, 2005.

[17] H. Hursti, Black Box Voting, "Critical Security Issues with Diebold TSx", May 11, 2006.

[18]A. Rubin, E. Felten, "Report Claims Very Serious Diebold Voting Machine Flaws," May 11, 2006. http://www.freedom-to-tinker.com/?p=1014

[19]D.W. Jones, "The Case of the Diebold FTP Site," Oct. 2, 2003. http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html

[20]T. Kohno, A. Stubblefield, A.D. Rubin, D.S. Wallach, "Analysis of an Electronic Voting System", July 24, 2003.

[21]RABA Innovative Solution Cell, "Trusted Agent Report: Diebold AccuVote-TS System", Jan. 20, 2004.

[22]"Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, Feb. 14, 2006.

[23]D.W. Jones, "Connecting Work on Threat Analysis to the Real World", June 8, 2006.

[24]A. Kerckhoffs, "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, Jan.-Feb. 1883.

[25]B. Schneier, "Secrecy, Security, and Obscurity," May 15, 2002.

[26]B. Schneier, "Voting Software and Secrecy," Oct. 2, 2006.

[27]J.H. Saltzer, M.D. Schroeder, "The protection of information in computer systems," *Proceedings of the IEEE* vol 63 no 9, Sept. 1975.

[28]D.S. Levine, "Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure," *59 Florida Law Review 135*. http://ssrn.com/abstract=900929

[29]D.L. Dill, B. Schneier, B. Simons, "Viewpoint: Voting and technology: who gets to count your vote?", Communications of the ACM, 46(8), Aug. 2003.

[30]A. Burstein, J.L. Hall, "Unlike Ballots, EAC Shouldn't Be Secretive," *Roll Call*, Jan. 22, 2007. http://josephhall.org/papers/Burstein_Hall-Roll_Call_2007-01-26.pdf.

[31]Notice of Rule Development, "Rule 1S-2.004: Procurement, Use and Assessment of Voting Systems," Florida Administrative Weekly, May 26, 2006.

[32]D. Dill, "Comments proposed rules 1S-2.004 and 1S-2.015," June 12, 2006. http://election.dos.state.fl.us/laws/proposedrules/pdf/partC_pubCom_r1s_2_004_2_015.pdf

[33]A. Yasinsac, "Comments on Rule #1S-2.004. Procurement, Use and Assessment of Voting Systems," June 10, 2006. http://election.dos.state.fl.us/laws/proposedrules/pdf/partA_pubCom_r1s_2_004_2_015.pdf

[34]R. Benham, "Proposed Rules 1S-2.004 and 1S-2.015," June 12, 2006. http://election.dos.state.fl.us/laws/proposedrules/pdf/partA_pubCom_r1s_2_004_2_015.pdf

Ms. LOFGREN. Next we have Mr. Hugh Gallagher, who is the managing director of Election System Acquisition and Management Services.

STATEMENT OF HUGH J. GALLAGHER

Mr. GALLAGHER. Thank you very much for giving me the opportunity to be here today.

I think you are hearing from this panel relative to this topic that there may sound like there is a divergence of opinion, when, in fact, I think we all agree that the number one thing we want is transparency in the process. We all concur on that, that we want the voters on election night to go home, go to bed knowing full well that the results of the election were fair, accurate and represent the will of the people.

What I would like to focus on is the concern—I concur with my colleagues to my right that open source code is probably something that is going to have to be considered, but the question is the context in which it is going to be considered. And so in keeping with Dr. Williams' thought process, one of the things I would like to look at is the common ground between all of the various groups that are here.

I believe, whether it is a third party at the State level or the Election Assistance Commission, I think we are needing to have an organization established that we might want to call the Voting Software Control and Distribution Board; an independent, trusted third party that would take possession of the source code and ownership of the source codes once that code has been approved by the respective ITAs. So once the vendor has released it to the ITAs for testing and certification, upon certification would go to the trusted third party supported by the National Institute of Standards and Technology, as an example, the idea being that the public would have access to this software under special controlled circumstances, probably not too dissimilar to what we see in the Library of Congress where there are historical records and information that you have to request, petition, go in and schedule to go in; a controlled environment in a single physical location where it can be monitored—where the activities can be monitored.

The process might look something like this, where the vendors, after they are done with their testing and certification process, notify the ITAs that once they are done and approved, they would go to the independent third party. The VSDC, the Voting Software Distribution Control Board, would take possession and configuration control. Vendors would be notified when clients require the software, and we might look at a process where this third party actually distributes the software independent of the vendors, and then the vendor has no contact with the final code once it leaves the ITAs.

There are a number of processes and details we would have to look at in terms of implementation, but I think what this does is start to bridge the concerns that both sides have, allows the access people are looking for, but not the free, unencumbered access, which I do think poses a risk in the public domain.

Thank you very much.

Ms. LOFGREN. Thank you.

[The statement of Mr. Gallagher follows:]

Testimony before the
Committee on House Administration
Election Subcommittee Hearing on Election Reform
March 15, 2007

Hugh J. Gallagher, Managing Director
Election Systems Acquisition & Management Services (ESAMS)

Introduction

Thank you for the opportunity to present testimony regarding the subject of open source software in electronic voting systems to the Committee. I have worked in the election industry for over ten years. I first entered this industry as Chief Operating Officer for a start-up company that was created to develop the next generation of direct record electronic (DRE) voting systems: In point of fact I was employee number 1. The product we developed was the first ever DRE to achieve dual NASED certification for software and hardware/firmware. For the last several years' I have been a subject matter resource to state and local governments on a variety of related election administration and technology issues. These experiences have given me a unique insight to the industry, its participants and technology.

Testimony

To begin, I believe that regardless of individual positions on the subject of open source software and by extension verifiable voter paper audit trails, a common goal exists: To make sure that when the American public goes to sleep on election night, they believe that the results of the election fairly represent the will of the people. From this mutual goal I believe all interested parties can find common and reasonable ground on how exactly to make this a continuing reality.

Regarding my position on the topic of open source software for electronic voting systems, I am appreciative of what proponents wish to accomplish. I recognize and acknowledge that a less than favorable perception exists regarding the voting system industry. However, in regards to open source code I can not at this time agree that such an approach would make our elections any more secure and reliable. I personally and professionally believe that requiring vendors to make their software open to public inspection would cause more harm than good. I believe this for the following reasons:

First, and potentially the most obvious is that by opening vendor software to public inspection invites precisely the kind of threat that many individuals believe is caused by the vendor software remaining proprietary: Unscrupulous individuals attempting to influence the election process. These individuals would be presented with a road map which could be used to circumvent system security, and as a direct result system reliability and accuracy. No where has empirical evidence been presented, or litigation substantiated, that vendor personnel have attempted to influence the election process by introducing malicious code. However, if the world of possible individuals having access to the voting system software now were open to the general public, what safe guards could be put in place to prevent malcontents from attempting to influence an election?

Arguments put forth by open source code proponents regarding electronic and physical safe guards built into election processes by election administrators have continuously

been dismissed. Therefore it would seem reasonable that if proponents state that an individual intent on causing mischief because of open source software must have access to the system, and they claim this is not possible due to these same electronic and physical safe guards which they had previously dismissed, then their entire argument to date as been moot – you can not have it both ways. I am not aware of any safety mechanism put forth by advocates to secure the integrity of the software, and by extension elections.

Continuing, under the "Attractive Nuisance Doctrine" of the law of torts, landowners can be held liable for injuries to children caused by a hazardous object, such as a simple swing-set or swimming pool that is likely to attract children, who are unable to appreciate the risk posed by the object. Is it difficult to envision an individual with more talent than common sense, being "attracted" to the open source code of an electronic voting system in order to see what they can do with it?

Recent literature and media accounts are replete with talented, mostly young individuals who took advantage of an inadvertent situation that was presented to them and subsequently found themselves involved in the game of "what can I get away with or do now that I have this information?" We have seen access to banking systems compromised as well as other interests, not to mention our own Department of Defense. Were these attacks and the mischief which resulted intentional or were they happenstance because an "attractive nuisance" presented itself? While I truly believe the proponents are honorable in their desire to ensure the public that through open

source software vendors are not manipulating the election process, can these same proponents make sure that rogue elements of the general public do not do what the vendors themselves have not done?

Are these proponents willing to personally assume the liability associated with a compromised election due to the attractive nuisance of open source software? The vendor community is at least finite in size and appropriate personnel screening and security techniques can be effectively implemented. Can we ensure similar screening and security techniques are applied to the general public? Would we as a public be willing to have our respective banks make public their financial and operations software? How would we react to our insurance companies doing so? Is the risk greater than the reward? I suggest it is.

Secondly, another obvious risk in open source software for voting systems is the loss of intellectual property and the competitive advantages it brings to its respective owner. The preponderance of voting system vendors are privately owned companies. These companies have historically been funded through private equity investment or venture capitalist – financing for new entrants with innovative technologies into the voting system market will follow this historic pattern. Venture capitalist and private equity funds traditionally want to maximize returns and minimize risks. One of the most important risks issues evaluated by such groups looking to invest is the security of intellectual property. In the voting system market place, vendor software represents the most significant part of their intellectual property.

The vendor's intellectual property represents for funding purposes a tangible asset; tremendous amounts of time and money go into protecting these assets as well as ensuring no infringements or compromise impact their potential value. If voting system vendor intellectual property rights on which they base so much of their value become public domain, where is the continued value-proposition for potential investors? What makes the voting system vendor an attractive investment opportunity at this point? How does the voting system vendor sustain its viability?

Hardware aspects of voting system vendors represents incremental advantage – most voting system vendors are not vertically integrated (i.e., own their manufacturing capabilities); fixed and variable costs of hardware do not allow in a competitive market high margins based on hardware alone. Without the protected intellectual property of software which gives the hardware the ability to perform, vendors have no competitive or distinct advantage in which to attract financing. Intellectual property has historically provided the basis for investors to place their resources at risk. Intellectual property is an integral part of value creation in <u>any</u> technology-based company and as such is a critical element in obtaining venture capital. If it is determined that voting system software is not entitled to be protected under the precepts of intellectual property rights, why not decide that the Federal Reserves software for managing money supply and interest rates be open to public inspection? It was developed by a third-party company; its' function is critical to ensuring stability in our country. What would the implications be if the Federal Reserves most intimate software systems were open to public inspection? Would such proponents be so cavalier with our money supply?

And finally, what is the express purpose of open source code for voting systems? Traditionally, advocates of open source code in the software industry cite several advantages to their position: 1) core software is free; 2) availability of the source code and the right to modify it; 3) the right to redistribute modifications and improvements to the code; and 4) the right to use the software in any way. How do these principals apply to voting system software? I suggest they do not. As stated before, I am not aware of any proposed safe guards or control mechanisms for protecting software in the public domain which has as critical a mission role as voting systems.

Conclusion

A report to the California Legislature on Open Source Software in Voting Systems dated January 2006 conducted by Secretary of State Bruce McPherson specially states impart "Open source advocates point to impressive accomplishments for software developed and maintained according to their principals, with apparent benefits to costs, efficiency, quality and security; however, upon close examination, the open source experience is more limited in scope and specific in application." None of the principals espoused by open source code proponents are even applicable to this situation. So the question remains: To what purpose does providing public access to vendor software benefit the public? Is the public in general proficient enough to understand the nuances of software development and subsequent coding to achieve requirements identified in voting system standards? No. How would the public know if there was "malicious code"

imbedded in the software? They wouldn't. Who specifically will be responsible for reviewing public code? I am not aware of any plan or organization or rules or bylaws or even secret-hand shakes as to how this would actually work. My inclination is to believe that it will be a "free-for-all." It stands to reason that under the proposed legislation requiring open source code for voting systems we will have a smorgasbord of opinion, insight, recriminations, professional disagreement, and more. Who will be the referee? Who will decide if something does or does not pass as reliable coding? As the saying goes you get ten economists in a room and you'll have ten different opinions; the same is true for software experts. Such public discourse and disagreement will do absolutely nothing to engender trust and confidence in the election process, and in fact will continue to erode confidence.

I support the findings presented in the California Legislature 2006 report: "A policy decision to require open source software for voting systems would disrupt existing voting systems without providing an immediate alternative." We must find an alternative that achieves the perceived goal advocates of open source code promote, without inducing highly unacceptable risk into the election process.

Consideration may be given to a compromise solution whereby an independent government agency, the Election Assistance Commission (EAC) supported by the National Institute of Standards and Technology (NIST), be designated as an escrow facility for all vendor software. The following procedures in principal may be considered:

1) Federal government scientist from NIST permanently serve as reviewers and controllers of such code on behalf of the American people;
2) All vendor software (source and compiled) tested and certified by the Independent Testing Authorities be delivered directly to the EAC;
3) Rigorous configuration management controls must be in place to ensure the integrity and the accuracy of the source and compiled code;
4) Vendors working with the EAC, would have required software directly delivered to a specific customer – at no time once the code has left the ITAs will the vendor have possession or access to that code;
5) Localities would take possession of application software for use in creating elections and programming machines;
6) EAC would conduct regular non-announced software configuration audits to localities; and
7) Detailed change control processes would be coordinated between vendors, ITAs, and the EAC to guarantee control of configurations.

Thank you,

I appreciate the opportunity to share with the Committee my thoughts on this particular matter. I am one of many voices you will hear on this and other related subjects. But as I mentioned in the beginning of my testimony, I believe all sides to this issue have a common goal we agree on. I am sure that a reasonable and acceptable compromise will be achieved to the benefit of all interested parties, but specifically the American people.

Respectfully:

Hugh J. Gallagher
Managing Director
Election Systems Acquisition & Management Services

Mr. Gallagher is a highly qualified Executive Manager, Technologist and Researcher with over 25 years' experience in technology based industries, most notably the Election Industry, to include subject matter expertise in, and research on the Help America Vote Act, and electronic voting systems and voter registration systems design, development, testing, certification, acquisition, implementation and training.

- Master of General Administration in Information Systems Technology and Marketing;
- Bachelor of Science in Business Administration & Economics;
- Over 10 years experience in the Elections Industry;
- Managing Director and founder of Election Systems Acquisition & Management Services;
- He is a certified internal ISO 9000 auditor;
- Designed and introduced a new Direct Record Electronic (DRE) voting system product which was the first in the industry to received dual certification from Federal testing and approval bodies;
- Developed all user-required product policies and procedures, training programs, logistics plans, security plans, configuration management plans, and QC plans for the implementation of the DRE voting system;
- Currently working with the Commonwealth of Virginia on design and implementation of its' new voter registration system – in particular in the redesign of associated workflow processes to implement required Federal and state legislation as it relates to absentee voting with particular focus on UOCAVA voters;
- Instructor for the Certified Elections/Registration Administrator (CERA) professional education program conducted jointly through the Election Center and Auburn University – instruct Module IV, Information Management & Technology in Elections & Voter Registration;
- Invited speaker on voting system and election policy issues at national and state conferences;
- Invited speaker at EAC public hearings on wireless voting system technologies (CALTECH);
- Worked with disabled community regarding accessibility issues for voting systems;
- Former U.S. Naval Officer;
- Research and Publications include: "Voting System Vendor and System Comparison," 2004; "Virginia Electoral Board Member Duties and Responsibility Handbook," 2004

Ms. LOFGREN. And, finally, we have Mr. Brian Behlendorf, who is the founder and CTO of CollabNet and also a director for Mozilla. So thank you for Firefox.

STATEMENT OF BRIAN BEHLENDORF

Mr. BEHLENDORF. I want to specifically talk about open source software a bit more, give you a background on it, and help you understand how it has really become essential to the software industry today, and where the issue of security lies with it, and how really it can be a big solution to that problem.

The software industry has seen a series of transformations throughout its brief history. The first transformation was initially called open systems, and this was the idea that we could build software that would run on multiple types of hardware, a fairly radical notion for its time.

The second major transformation was called open standards. This was the idea that companies could get together and talk about common data formats, common protocols to share data and build systems that, by talking to each other, build greater value for customers and for the industry as a whole.

Both of these transformations were disruptive transformations. Some of these companies grew and benefited from them, among them Microsoft, Sun, and Cisco; other companies resisted and in some cases perished.

The third major transformation in this linear series of transformations is open source software. Open source software is software defined as being licensed under a very generous copyright license, licenses that allow many kinds of use at zero price, provide access to the underlying source code, allow modification and improvement by recipients, and allows those recipients the right to share those improvements with others. This approach can result in fewer defects, greater flexibility, more rapid innovation and a more competitive marketplace than the proprietary alternatives.

Today every major technology vendor releases some portion of its intellectual property under an open source license. The business models behind this investment are a mixture of support services and strategic opportunities for other proprietary offerings. Sun, HP, and IBM all have significant revenue streams based on open source software. Even Microsoft has acknowledged the value on open source by releasing some minor software under such a license.

On the customer side, open source software is used everywhere from critical Wall Street financial systems where security is paramount, and the teenage hackers and terrorists would be just as attracted, to such commodity devices as cell phones and TiVos. Within the public sector, we see open source used today in the Pentagon, in the Departments of Commerce, Energy, and Homeland Security. In all of the above examples, open source and transitional proprietary software can peacefully coexist.

Is open software guaranteed to be more secure? No. It is challenging for even the most competent engineers to write a secure code. The only widely recognized indisputable method to designing and building highly secure systems is massive developer peer review. The more widely inspected a code is, the smaller the chance of undiscovered defects. This extends to the development process

itself. The larger the development team around a given body of code, and the more the deliberations of that team are open to the outside world, the more reliable their designs are likely to be.

This community approach is the key ingredient in any successful and secure open source project.

In the interest of time, I will point your attention to the open SSL project example that I give in the written testimony.

Finally, the most useful aspect to choosing an open source project is the inherent protection it can give against vendor log-in. Customers can switch vendors without surrendering any legal rights to use and extend the software. Thus, open source is a new kind of relationship between customer and vendor from one of dependency to one of cooperation.

To summarize, open source in the software industry today is accepted, it is real, it is probusiness and procustomer, and it has a tremendous chance to build trust and security and proper operation of voting system software.

[The statement of Mr. Behlendorf follows:]

WRITTEN TESTIMONY OF BRIAN BEHLENDORF
CHIEF TECHNOLOGY OFFICER
COLLABNET
BEFORE THE COMMITTEE ON HOUSE ADMINISTRATION, ELECTIONS
SUBCOMMITTEE
U.S. HOUSE OF REPRESENTATIVES
MARCH 15, 2007

Members of the Committee, good afternoon and thank you for the opportunity to speak to you this afternoon on the topic of "disclosed" and Open Source software. My name is Brian Behlendorf. I am the Founder of CollabNet, a global company focused on providing tools and services for collaborative software engineering, as best exemplified by the Open Source software community. For the last 8 years I have served as its Chief Technology Officer and Executive Board member.

Today I'm going to talk about how Open Source is the continuation of a series of transformations that have taken place in the software industry. I'll explain how it has become a dependable mechanism for software development and commerce, how it can lead to more secure and trustable software, and how it serves the interests of the customers by reducing vendor lock-in. I'll also explain the real differences between Open Source and simply "disclosed" software, an understanding that is critical as you look at the language of proposed legislation.

To further explain my context for these comments, I was a co-founder and the first President of the Apache Software Foundation, a U.S.-based 501c3 nonprofit organization responsible for the technology used in over 60% of the web sites in existence today. Currently I serve on the Executive Board of the Mozilla Foundation, the organization responsible for the Firefox web browser. I also served for three years on the initial Executive Board of the Open Source Initiative, the organization responsible for the defining the "Open Source" trademark and educating the public on the concept. I speak today on my own behalf.

The software industry has seen a sequence of deep and often disruptive transformations throughout its brief history, with each transformation creating new opportunities and new industry leaders. The first major transformation, in the 1970s and 1980s, was called "Open Systems", which promoted the unorthodox notion that software should be built that could run on different kinds of hardware. Microsoft was born during this transformation and profited tremendously from its premise, as did many other software companies we know of today. Some other companies, such as IBM, adapted to the changing environment, survived, and thrived. Others resisted the move, and perished.

The second major transformation, which came to prominence in the early 1990s and yet is still underway, was that of "Open Standards". The unorthodox notion this time was that two companies, ten companies, or more could meet as peers and create common vocabularies for interchanging data between different pieces of software. The greater the number of software programs that used this common vocabulary, the greater the total amount of value created. From this concept was born the Internet, the network of networks, made possible only by the principle of sharing a common network vocabulary (called TCP/IP) as widely as possible. As with the first transformation, we saw new companies like Cisco and Sun emerge, we saw other existing companies adapt and thrive, and we saw others resist and perish.

The third major transformation to have taken place in the software industry is that of "Open Source" software. Open Source software is software licensed under a generous copyright license; licenses that allow many kind of use at zero price, that provide access to the underlying application "source code", that allow modification and improvement, and that allow the recipient the right to share their modifications with others. Here, the unorthodox notion is that this approach can result in fewer defects, greater flexibility, more rapid innovation, more responsive vendors, and a more competitive marketplace than the more proprietary alternatives.

Today, every major technology vendor releases some portion of its intellectual property under an Open Source license. The business models these companies pursue to justify such an investment are a mixture of support, services, and strategic opportunities created for other proprietary offerings. Red Hat is the most famous example of this, commanding a market capitalization of over $4B. Traditional technology companies have embraced this too: Sun, HP, and IBM all have significant revenue streams based on Open Source software. Even Microsoft has acknowledged some value to this approach, not just by partnering with Novell to co-sell Linux to Microsoft customers, but by also releasing some small Open Source projects themselves.

On the customer side, Open Source software has crossed the chasm from its early adopter support amongst the engineers to enterprise production use. Every firm on Wall Street I have talked to depends upon Linux and other Open Source software to execute trades or conduct other financial transactions. Many consumer devices invisibly embed Open Source technologies, from cell phones to Tivos to automobile electronics. Within the public sector, the use of Open Source software has grown tremendously, in such demanding agencies as the Pentagon, Commerce, Energy, and Homeland Security. In all these environments, Open Source software and proprietary software can co-exist, thanks to open standards and open systems.

Is Open Source software guaranteed to be more secure? In software, as anywhere else, there are no guarantees. It is extremely challenging for even the most competent engineers to write invulnerable code - it's as likely as planting and managing a garden that has no weeds. New methods of attack are discovered all the time, and the re-use of software in new settings can often open new holes. Yet the ability to prevent mistakes or external compromise in certain situations, such as electronic voting systems, is critical.

The only widely recognized indisputable method to achieve low-defect software is developer peer review. Eric Raymond, the author of The Cathedral and the Bazaar, a paper that first popularized the concepts around Open Source software, once said, "To enough eyeballs, all bugs are shallow." The more widely inspected code is, the lesser the chance of the undiscovered defect. This extends to the development process itself - the larger the development team around a given body of code, and the more that the deliberations of that team are opened to the outside world, the more reliable their designs are likely to be. This "community" approach is the key ingredient to any successful Open Source project.

An illustration of this is the OpenSSL project. Launched over 12 years ago, this is a library of cryptographic routines and tools and functionality that is used to secure everything from credit card and other sensitive transactions over the Internet, to "smart cards" for accessing physical systems. This library has become the reference platform for building cryptographically secure applications. Written by individuals working around the world, this library has received extensive scrutiny from security professionals and researchers worldwide, and has gained FIPS-140 certification for use in U.S. government applications. Like any piece of software, there are bugs, and occasionally one is found and

reported to the development team. Rather than deny the existence of such a bug, the public nature of the project forces them to embrace that discovery, fix it as quickly as possible, and issue an update - often within a matter of hours, almost always within a few days. This level of scrutiny, and the degree of responsiveness, has built confidence in the hearts and minds of security professionals everywhere in OpenSSL.

If this were a commercial product forced merely to "disclose" its source code with carefully selected partners in a closed manner, the chances of a community forming to review that work effectively and sufficiently to gain that same level of trust, are close to zero. This is why the security and effectiveness of an "Open Source" system is not merely about "disclosure", but about co-development between peers, and the creation and promotion of common technologies to solve common problems.

Finally, the most useful aspect to choosing an Open Source product is the inherent protection it can give against vendor lock-in. A support customer of one Linux vendor, has the freedom to shift to another Linux vendor should they become dissatisfied with the first. The customer's investment of training time on Linux, improvements to Linux, and in technology on top of Linux, does not have to be thrown away should the commercial relationships change. Open Source allows the redefinition of the traditional relationship between customer and provider, from one of dependency towards one of enablement and cooperation.

Customers of vendors selling Open Source electronic voting software necessarily retain the legal rights to continue to use and improve the software, even if they elect to switch to another vendor. The vendors will continue to have a lucrative market to pursue - that of providing and maintaining the election hardware, the customization of the software to each precinct's needs, and providing support services before, during, and after the election. Such activities are complex enough to create plenty of opportunity for relative competitive advantage for each vendor. Further, each vendor's R&D costs would be reduced, as the development of common software is shared between multiple vendors, and could involve volunteers, non-profit organizations, or government-funded contributors. Viable Open Source software designed for voting systems already exist, and have been used in elections in Australia, though no such system has yet been deployed in the United States.

To summarize, the Open Source transformation taking place in the software industry today is real, it is pro-business and pro-customer, and it has a tremendous chance to build trust in the security and proper operation of such software. It alone can not guarantee a trustable electoral process, but in conjunction with other solutions it can play a key enabling role. And along the way, it can help redefine the relationship between the public sector and the system vendors in favor of the public interest.

Thank you again for allowing me to testify.

Brian Behlendorf

Ms. LOFGREN. Thanks to all of you for excellent and interesting testimony.

Again, I will try—each of us will try to limit our questions to the same 3 minutes that you have given to us.

Let me start with Mr. Gallagher. The EAC Commissioner, I understand, has said that disclosing source codes would help to restore public trust in the election process. And he explicitly stated vendors should not have the right to keep a source code a secret. He has called on computer scientists and election officials to work together to solve many of the problems related to voting systems, and I think in some cases it can be either problems, or perceptions of problems are very damaging as well.

How do you respond to that explicit call from the EAC?

Mr. GALLAGHER. First of all, I have tremendous respect for Commissioner Soaries. He is a great man, and a great public speaker if you have ever heard him.

I don't think we are at odds here. I don't think anybody at this table is potentially at odds. I think we agree there should be some degree of openness. The question is in what circumstances; how does that actually work; what are the mechanics?

I would submit that having things, as I understand it, and I may be wrong—that in a true open source environment, software environment, my particular concern is one of the attractive nuisance; in other words, persons coming along who might not otherwise be inclined for mischief all of a sudden seeing and being presented with an opportunity, not too dissimilar from my children, and wanting to exploit that opportunity to nefarious ends, or even just for grins and giggles.

I think what we want is an open source environment controlled in some form or fashion, agreed-upon rules and procedures that everyone can subscribe to, because, as my colleague to my left was saying, that the more people involved, the better that withstands the test. The only question I would ask is what are the rules, because if you get too many cooks in the kitchen, you get too many recipes.

Ms. LOFGREN. I wonder, Dr. Wagner, if you could comment on Mr. Gallagher's statement, and also if you could—I don't know if this is to the business school or the computer science school, but if—the defects are going to be probably one of two kinds: either an intentional backdoor or a bug that was not intentional. And presumably the intentional backdoor is more easily found and resolved. Maybe not. But if we were to do an open source regime, as suggested by Mr. Behlendorf, what would the economic impact be? Would it be adverse on vendors of machines? Could they accommodate it and still flourish? What do you think the impact would be?

Mr. WAGNER. So to the first of your questions, I think in the long run, until we disclose all of the source codes to the public, I believe that the public will be—will have concerns, will not trust and will express reservations over the source code. So in the long run, I believe that is where we need to head to enable the public and the candidates to gain confidence.

As far as the economic impact of source code disclosure, I believe that there are some costs to source code disclosure, but that is eas-

ily manageable, especially through a gradual introduction of increasing disclosure.

Ms. LOFGREN. My time has expired. So I will ask the Ranking Member to ask his questions.

Mr. MCCARTHY. I apologize. I want to be quick and maybe try to get some yes or no answers.

I would appreciate it if we could get everybody's cards. I would like to talk to you later.

First to Dr. Wagner, you were part of the FSU team that analyzed down there. Did you have the source code?

Mr. WAGNER. Yes.

Mr. MCCARTHY. And maybe to Mr. Zimmerman, you had mentioned in Fedder v. Gallagher—I read your statement here where you go through it. You state, with regard to your lawsuit with these Sarasota voters, that Florida prevented independent inquiry into the source code. Do you still keep that same statement after the FSU Study?

Mr. ZIMMERMAN. Yes, I do. And with all due respect to David Wagner, who I have worked with in the past many times, I think he is a very fantastic scientist who I go to for information from time to time.

Mr. MCCARTHY. You have used him before?

Mr. ZIMMERMAN. In an informal way, yes.

Mr. MCCARTHY. But you feel this is not an honest——

Mr. ZIMMERMAN. What has gone on in the Fedder v. Gallagher case, is essentially the State is deciding on its own the scope of a project, and I don't even believe Mr. Wagner will say it is an expansive project that is aimed at getting all of the—find all of the potential problems and——

Mr. MCCARTHY. I understand. I don't want to get into the case because I can't go through the cases. But just on the study itself, do you feel that study—you don't agree with the study even though he stated he had the source code?

Mr. ZIMMERMAN. I believe that there are problems with the study, yes, and I would be happy to talk with you later.

Mr. MCCARTHY. Okay. Thank you. And Mr. Williams. So your statement—and it was kind of towards the end—you had concerns with hackers, with others. If you just put them all out there, you thought maybe testing them much like maybe the FSU study would be the proper way? I don't want to put words in your mouth, but am I understanding that correctly?

Mr. WILLIAMS. I am very much in favor of controlled evaluation of source code. I am very much opposed to just opening up the kimono, okay, because not just hackers and terrorists but well-meaning—most of our problems are not caused by bad guys. They are caused by well-meaning good guys. So there is no advantage to making it possible for any citizen to modify voting system software.

We don't operate voting systems that way. You get a voting system as solid as you can get it, and you freeze it. You don't let anybody touch it. If anybody touches it, you make it go back through the entire sequence of tests again. So there is no advantage from that point of view of being able to modify and expand and customize it to your own use. That is not what we do with voting system software. The only advantage is to be able to find these sup-

posed bugs and Trojan horses and all the bad stuff, and I think that people like Dr. Wagner can do that in a controlled situation just as well as he can with an open situation.

Mr. MCCARTHY. Only because you are both Ph.Ds. Have you had an opportunity to read the FSU study?

Mr. WILLIAMS. I have read most of it.

Mr. MCCARTHY. Do you agree with Mr. Zimmerman that you think something is wrong with the study?

Mr. WILLIAMS. Well, I won't agree or disagree but I will make a statement about the study. In my 20 years of doing this kind of evaluation, that is the most open, professional well-written study I have yet to see.

Mr. MCCARTHY. All right. Thank you. I appreciate it. You are very interesting.

Ms. LOFGREN. Our last member is Susan Davis, who will have her questions answered.

Mrs. DAVIS. Thank you. Thank you, Madam Chair. Thank you all for being here. I think this question would really go to you, Dr. Wagner. Have they tested all the systems in Florida to your knowledge? And could you help us understand how that was done and what should have been done perhaps or going forward, what we ought to be looking at?

Mr. WAGNER. Certainly. Well, I can't speak for the state of Florida. I can't speak for the entire audit they did. The team that I was involved with had a narrow mandate to look to see whether there were problems in the machine software provided to us that could have caused or created the undervote in that race there. And our conclusion was that it did not.

Now, I can understand why some members would be—why there may be some folks who would be reluctant to trust the results of our study. Until everyone can choose the expert of their own choosing, I can understand why they may have concerns.

Mrs. DAVIS. Now as part of your all—were you able to go back and see the testing that had been done?

Mr. WAGNER. We were not asked to review the entire Florida State audit, we had a very specific mandate.

Mrs. DAVIS. Okay. Thank you. Thinking about how the public responds. I mean, this is really all about the credibility of the systems, and whether or not if you had transparency, is there a concern that some individuals with some knowledge could actually frighten the public into believing that there were flaws in the system that could not be overcome? And how would that work?

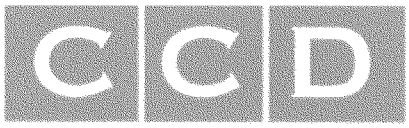
Mr. WAGNER. I think there is some concern there in the short term, given my experience of how full of security problems these machines are. In the short term, that would be a concern. I think that the way to address that is through a gradual transition planning where in the beginning, we begin by following Professor Williams's recommendations to make the source code available to qualified experts, give the vendors a chance to address those problems, and prepare their systems for disclosure and gradually move towards a long-term goal of public disclosure.

Mr. WILLIAMS. I think it is worth pointing out that the vendor in this case was a full participant in this study. Is that a fair statement?

Mr. WAGNER. I was pleased with their cooperation, yes.

Ms. LOFGREN. This has been a very helpful panel. And obviously, your written testimony amplifies considerably on your oral testimony today. It is very, very helpful. I know it is not easy to wait for the Congress Members to come over from an extended vote and then of course to shorten because now we are terribly behind. But we do appreciate this, and it does make a difference in our understanding and hopefully our wisdom as we proceed. So thank you each and everyone. It is very much appreciated. And with that, this hearing is adjourned.

[Whereupon, at 3:30 p.m., the subcommittee was adjourned.]



CONSORTIUM FOR CITIZENS
WITH DISABILITIES

Rights Task Force Position on Voting Machine Security and Voter Verified Paper Audit Trails (VVPAT)

The Consortium for Citizens with Disabilities (CCD) is a coalition of more than 100 national disability organizations working together to advocate for national public policy that ensures the self determination, independence, empowerment, integration and inclusion of children and adults with disabilities in all aspects of society. The Rights Task Force of CCD focuses on civil rights and protections for people with disabilities, and the enforcement of those rights and protections by federal agencies.

The expertise and primary interest of CCD lies in matters of equal access and the rights of people with disabilities. As it pertains to voting, this involves specifically ensuring enforcement and protection of the rights guaranteed under the Help America Vote Act (HAVA) and other applicable federal law. CCD does not have a blanket policy either for or against Voter Verified Paper Audit Trails (VVPAT) or other means of independent vote verification. CCD seeks to ensure that any and all measures instituted to provide enhanced security, accuracy and/or voter confidence must be developed and implemented in a manner that ensures immediate accessibility for people with disabilities. Such measures must not interfere with the current ability of voters with disabilities to cast private and independent ballots, as mandated by HAVA and should focus on enhancing security and accessibility rather than promoting one system over another. This will allow for continued improvement of available technologies, while maximizing accessibility and security options available to voters with disabilities in the future.

The disability community shares the interest of all Americans in ensuring that elections are fair, secure and accurate. The position of CCD is that if a paper audit trail or other means of independent vote verification is used in any jurisdiction, then the means of vote verification must be accessible to all individuals with disabilities at the same time as the requirement goes into effect for all voters. Accordingly, CCD would oppose any paper audit trail or other means of independent vote verification requirement that does not meet this standard.

For questions about this position, contact
one of the following Rights Task Force Co-chairs:
Janna Starr at jstarr@ucp.org or Day Al-Mohamed at dalmohamed@acb.org

1660 L Street, NW, Suite 701 • Washington, DC 20036 • PH 202/783-2229 • FAX 783-8250 • Info@c-c-d.org • www.c-c-d.org

ELECTRONIC VOTING MACHINES PROMISE TO MAKE

FIXING THE VOTE

ELECTIONS MORE ACCURATE THAN EVER BEFORE, BUT ONLY IF CERTAIN PROBLEMS—WITH THE MACHINES AND THE WIDER ELECTORAL PROCESS—ARE RECTIFIED

By Ted Selker

Voting may seem like a simple activity—cast ballots, then count them. Complexity arises, however, because voters must be registered and votes must be recorded in secrecy, transferred securely and counted accurately. We vote rarely, so the procedure never becomes a well-practiced routine. One race between two candidates is easy. Half a dozen races, each between several candidates, and ballot measures besides—that's harder. This complex process is so vital to our democracy that problems with it are as noteworthy as engineering faults in a nuclear power plant.

Votes can be lost at every stage of the process. The infamous 2000 U.S. presidential election dramatized some very basic, yet systemic, flaws concerning who got to vote and how the votes were counted. An estimated four million to six million ballots were not counted or were prevented from being cast at all—well over 2 percent of the 150 million registered voters. This is a shockingly large number considering that the decision of which candidate would assume the most powerful office in the world came to rest on 537 ballots in Florida.

VOTING MACHINE—here, Sequoia Voting Systemss' Edge AVC Edge (*right*)—is fairly typical of direct record electronic (DRE) voting machines on the market. Voters enter their votes via a touch-screen interface (*left; screen shot from TK TK*).

Three simple problems were to blame for these losses. The first, which made up the largest contribution, was from registration database errors that prevented 1.5 million to three million votes; this problem was exemplified by 80,000 names taken off the Florida lists because of a poorly designed computer algorithm. Second, a further 1.5 million to two million votes were uncountable because of equipment glitches, mostly bad ballot design. For example, the butterfly ballot of Palm Beach County confused many into voting for an unintended candidate and also contributed to another appalling outcome: 19,235 people, or 4 percent of voters, selected more than one presidential candidate. Equipment problems such as clogged punch holes resulted in an additional 682 dimpled ballots that were not counted there. Finally, according to the U.S. Census Bureau, about one million registered voters reported that polling-place difficulties such as long lines prevented them from casting a vote.

Thus, registration and polling-place troubles accounted for about two thirds of the documentable lost votes in 2000. The remaining one third were technology-related, most notably ballot design and mechanical failures. In the aftermath of the 2000 election, officials across the country, at both the federal and local levels, have scrambled to abandon old approaches, such as lever machines and punch cards, in favor of newer methods. Many are turning to electronic voting machines. Although these machines offer many advantages, we must make sure that these

new systems simplify the election process, reduce errors and eliminate fraud.

Some countries have introduced electronic systems with great success. Brazil started testing electronic voting machines in the mid-1990s and since 2000 has been using one type of machine across its vast pool of 106 million voters. It has multiple organizations responsible for different aspects of voting equipment development as part of the safeguards. It also introduced the machines in carefully controlled stages—with 40,000 voters in 1996 (7 percent of whom failed to record their votes electronically) and 150,000 in 1998 (2 percent failure). Improvements based on those experiments reduced the failure rate to an estimated 0.2 percent in 2000.

Voting Technology

VOTING SYSTEMS have a long history of advancing with technology. In ancient Greece, Egypt and Rome, marks were made for candidates on pieces of discarded pottery called ostraca. Paper superseded pottery in the hand-counted paper ballot, which is still used by 1.3 percent of U.S. voters. Other modern technologies are lever machines, punch cards and mark-sense ballots (where each candidate's name is next to an empty oval or other shape that must be marked correctly to indicate the selection, and a scanner counts the votes automatically). The table on pages 94 and 95 summarizes the benefits and drawbacks of each of these methods and suggests ways to improve them. A lengthier discussion of nonelectronic systems is at www.sciam.com/ontheweb.

Electronic voting machines have been around for 135 years—Thomas Edison patented one in 1869. Elections started testing electronic voting machines in the 1970s, when displaying and recording a ballot directly into a computer file became economical. At first, many were mixed-media machines, using paper to present the selections and buttons to record the votes. Officials had to carefully align the paper with the buttons and indicator lights. Electronic voting machines that use such paper overlays are still on the market. More modern Direct Record Electronic (DRE) voting machines present the ballot and feedback information on an electronic display, which may be combined with audio.

Such machines have many advantages: they can stop a voter from choosing too many candidates (called overvoting), and they can warn if no candidate is picked on a race (undervoting). For instance, when Georgia changed over to DREs in 2002, residuals (the total of overvotes and undervotes combined) were reduced from among the worst in the nation at 3.2 percent on the top race in 2000 to 0.9 percent in 2002. So-called ballotless voting allows the machines to eliminate tampering with physical ballots during handling or counting. (Lever machines, dating back to 1892, share many of those features.)

Yet the birthing of DRE voting equipment in the U.S. has not been easy. The voting machine industry is fragmented, with numerous companies pursuing a variety of products and without a mature body of industry-wide standards in place. Deciding what is a good voting machine is still being discussed by various advocacy organizations and groups such as the IEEE Project 1583 on voting equipment standards. Allegations of voting companies using money to influence testing and purchasing of equipment are not uncommon.

Complicating matters, local jurisdictions across the country have different rules and approaches to testing and using voting equipment. Some counties, such as Los Angeles, are sophisticated enough that they commission voting machines built to their own specifications. many other municipalities know so little about voting that they employ voting companies to run the election and report the results.

Polling-place practices add further hazards of insecurity and potential malfunctions. I recall walking into the central election warehouse (where the voting machines are stored and the precinct vote tallies are combined) in Broward County, Florida, when it was being used for a recount in December 2002. The building's loading dock was opened to the outdoors for ventilation. The control center for tallying all the votes was a small computer room; the door to that room was ajar and no log was kept of personnel entering and leaving.

Beyond external issues, DRE machines themselves have had technological shortcomings that have slowed their adoption. Voters have found their displays confusing or challenging to use. Software bugs and difficulties in setting up DREs have also presented problems. During the 2002 Broward County recount, I was allowed to try out machines from Electronic Systems and Services (ESS), one of the country's major election machine makers. The ESS machines had an excessive undervote because the "move to next race" button was too close to the "deposit my ballot" button. An audio ballot was so poorly designed it took about 45 minutes to vote.

On machines made by the company Sequoia, people who chose a straight party vote and then tried to select that party's presidential candidate were unaware that they were *deselecting* their presidential choice. A massive 10 percent undervote was registered in one county using Sequoia machines in New Mexico.

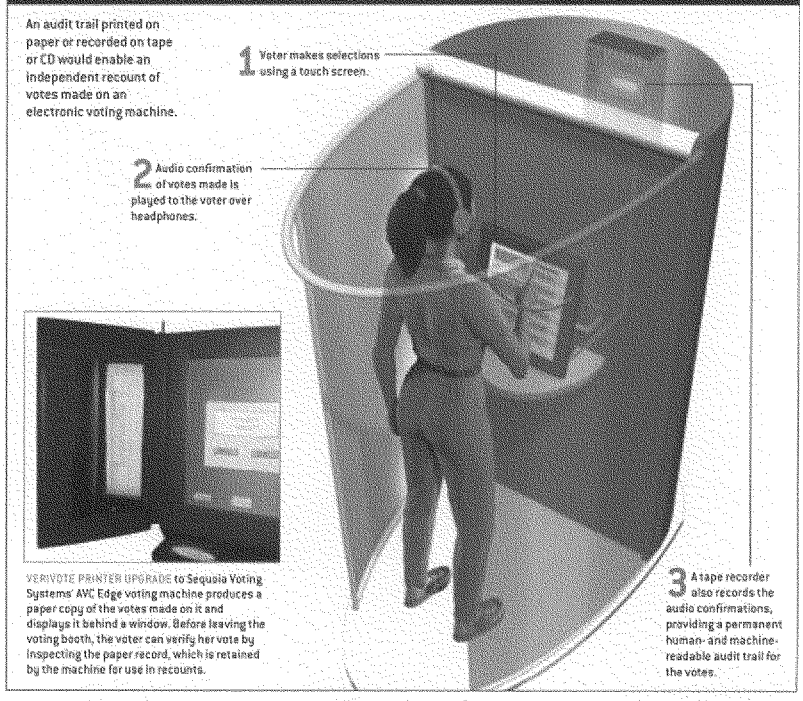
Examining the insides of new voting machines still reveals

Overview/*Electronic Voting*

- Following the infamous 2000 presidential election, electoral officials around the country have scrambled to upgrade their voting technology with newer systems, such as direct record electronic voting machines (DREs).
- A state or county that is considering buying DREs, should hire experts to test the machines thoroughly for bugs, malicious software and security holes and to assess the quality of the user interface.
- Election officials and polling-place workers should be well versed in the operation of their machines and should follow practices that do not compromise the security of the vote.
- In addition to these technology-related issues, the voter registration process and polling-place practices in general must be improved to prevent massive losses of votes.

AUDIT TRAILS

An audit trail printed on paper or recorded on tape or CD would enable an independent recount of votes made on an electronic voting machine.



VERIVOTE PRINTER UPGRADE to Sequoia Voting Systems' AVC Edge voting machine produces a paper copy of the votes made on it and displays it behind a window. Before leaving the voting booth, the voter can verify her vote by inspecting the paper record, which is retained by the machine for use in recounts.

many physical security faults. For example, some machines have a lifetime electronic odometer that is supposed to read every vote that the machine makes. But the odometer is connected to the rest of the machine by a cable that a corrupt poll worker could unplug to circumvent it without breaking a seal.

Source code for voting machines made by different companies, like most commercial software, is a trade secret. Election machine companies allow buyers to show the source code to experts under confidential terms. Unfortunately, the local election officials might not know how to find a qualified expert. And when they find one, will the voting companies be required to listen? For instance, in 1997 Iowa was considering a voting machine made by Global Election Systems, which was later bought out by Diebold. Computer scientist Douglas W. Jones of the University of Iowa pointed out security issues, and the state bought Sequoia machines instead. In February 2003 Diebold left its software on unsecured servers, and DRE critics posted Diebold's code on the Internet for everyone to see. The problems that Jones saw six years earlier had not been fixed. Any person with physical access to the machines and a moderate amount of computer knowledge could have hacked into them to produce any outcome desired.

The best computer security available depends on sophisticated encryption and carefully designed protocols. Yet to know the system has not been compromised requires testing. DRE machines have not received the constant testing that they require. Security of today's voting machines is wholly dependent on election workers and the procedures that they follow.

Because virtually all tallies, no matter what voting method is used, are now stored and transmitted in some electronic form, computer fraud is possible with all voting systems. The advent of DRE machines potentially allows such tampering to go

Jodi Hilton (illustration); Jim Wehtje (photographs)

EXISTING VOTING TECHNOLOGIES

Improving or optimizing an existing technology may be a better choice for many counties than hasty adoption of a new system—introduction of a new technology is often accompanied by an increase in errors.

TECHNOLOGY	Hand-counted paper ballots	Lever machines	Punch cards
COMMENTS	▪ Used by 1.3 percent of U.S.	▪ First used in 1892 in Lockport, N.Y.	▪ First used in 1964 in Fulton and De Kalb counties, Georgia
ADVANTAGES	▪ Simple ▪ Lowest residual[1] rate	▪ Overvotes[1] are impossible ▪ Guarantees secrecy of vote	▪ Removes human errors of tallying ▪ Compact machines
DISADVANTAGES	▪ Recounts differ from original count by twice as much as machine-counted votes do ▪ Persistent allegations of votes being altered, added, lost, and so on	▪ Bulky, massive machines ▪ Defective odometers: common ▪ Misreading of odometers ▪ Voting falloff on lower races (for Senate, state office, for example)	▪ Hard to punch holes correctly ▪ Often punch wrong hole ▪ Ballot design troubles ▪ Card readers jam frequently
WAYS TO IMPROVE	▪ Count by mechanical scanner ▪ Treat paper with light, heat or coating material to make vote indelible	▪ Check and service beforeeach election ▪ Monitor odometers with video cameras ▪ Improve labeling of groups of levers forming a race ▪ Adjustable height of machines	▪ Optical way to check ballot while in booth might help

ELZA IERNETT

unchecked from the point at which the voter attempts to cast a ballot. Schemes for altering ballots have always existed, but a computerized attack could have widespread effect were it waged on a large jurisdiction that uses one kind of software on one type of machine. Using a single system allows large jurisdictions to get organized and improve their results but must be accompanied by stringent controls.

The successful reduction of residuals across all of Georgia, mentioned earlier, is a case in point. Thorough tests on the DREs at Kenisaw State University found many problems, which were resolved before the machines were put into use. This rigorous testing and careful introduction of the machines were central to the state's success.

Electronic Fraud

HOW CAN WE FIND all the dangers created by bad software and prevent or correct them before they compromise an election? Reading source code exposes its quality and its use of security approaches and can reveal bugs. But the only completely reliable way to test software is by running it through all the possible situations that it might be faced with.

In 1983 Ken Thompson, on receipt of the Association for Computing Machinery's Turing Award (the most prestigious award in computer science), gave a lecture entitled "Reflections on Trusting Trust." In it he showed the possibility of hazards such as "Easter eggs"—pieces of code that are not visible to a reader of the program. In a voting machine, such code would do nothing until election day, when it would change how votes were recorded. Such code could be loaded into a voting machine in many ways: in the voting software itself, in the tools that assemble the software (compiler, linker and loader), or in the tools the program depends on (database, operating system scheduler, memory management and graphical-user-interface controller).

Tests must therefore be conducted to catch Easter eggs and bugs that occur only on election day. Many electronic voting machines have clocks in them that can be set forward to the day of the election to perform a test. But these clocks could be manipulated by officials to rerun an election and create bogus voting records, so a safer voting machine would not allow its clock to be set in the field. Such machines would need to be tested for Easter egg fraud on election day. In November 2003 in California a random selection of each electronic voting system was taken aside on the day of election, and careful parallel elections were conducted to show that the machines were completely accurate at recording votes. These tests demonstrated that the voting machines were working correctly.

To prepare for a fraud-free voting day requires that every effort be made to create voting machines that do not harbor malicious code. The computer science research community is constantly debating the question of how to make provably secure software. Computer security experts have devised many approaches to keep computers reliable enough for other purposes, such as financial transactions. Financial software transfers billions of dollars every day, is extensively tested and holds up well under concerted attacks. The same security techniques can be applied to voting machines. Some researchers believe that the security precautions of "open source" (making the programs available for anyone to examine) and encryption techniques can help but not completely guard against Easter eggs.

Guarding votes against being compromised has always re-

Mark-sense ballots	Electronic machines	Internet voting, phone messaging, interactive TV
■ First used in 1962 in California	■ First used in 1975	■ Internet voting first used in 2000 primary Phoenix, Ariz.
■ With in-precinct scanning, has lowest residuals of any mechanical method ■ Easier than punching holes ■ Voter can read candidates right on ballot	■ Overvotes are impossible ■ No human errors of tallying ■ Easy for people with physical disabilities to use ■ Good feedback	■ Vote from home ■ People with physical disabilities can use their own special-needs setup ■ No human errors in tallying
■ Ballot readers are slower, harder to calibrate and more prone to jamming than card readers ■ Bulky ballot ■ Ballot easy to spoil	■ User interface often poor ■ Concerns about malicious software ■ Concerns about computer obsolescence	■ Concerns about malicious software, network problems and hackers
■ Use an in-precinct scanner to catch problems and give the voter a second chance to vote ■ Use DRE to mark ballot ■ "Fill in the shape" version better than "connect the arrow" version	■ Test ballots ■ Consider closed systems ■ Test system, including on day of election	■ Use special Web browser ■ System on a CD ■ New approaches to security needed, such as multiple software agents

*Residual: an undervote or an overvote. (Overvote: voting for too many candidates in a race. (Undervote: voting for too few candidates in a race.)

quired multiple human agents watching each other for mistakes or malice. The best future schemes might include computer agents that check one another and create internal audits to validate every step of the voting process. The Secure Architecture for Voting Electronically (SAVE) at the Massachusetts Institute of Technology is a demonstration research project to explore such an approach. SAVE works by having several programs carry out the same tasks, but while using such different methods that each program would have to be breached separately to compromise the final result. The system knows to call foul when too many modules disagree.

Audit Trails

SOME CRITICS INSIST that the best way to ameliorate such attacks is by providing a separate human-readable paper ballot. This widely promoted scheme is the voter-verified paper ballot (VVPB) suggested by Rebecca Mercuri, then at Bryn Mawr College. The voting machine prints out a receipt, and the voter can look at it after voting and assure himself that at least the paper records his intention. The receipt remains behind a clear screen so no one can tamper with it during its inspection, and it is retained by the machine. If a dispute about the electronic count arises, a recount can be conducted using the printed receipts. (It is not a good idea for the voter to have a copy, because such receipts could encourage the selling of votes.)

Although the VVPB looks quite appealing at first glance, a deeper inspection exposes some serious flaws. First, it is complicated for the voter. Elections in this country often have many races. Validating all the selections on a separate paper after the ballot has been filled out is not a simple task. Experience shows that even when confronted with a printout that tells voters in which race they have made a mistake, few are willing to go back and correct it. Anything that takes a voter's attention away from the immediate act of casting a ballot will reduce the chances of the person voting successfully. Every extra button, every extra step, every extra decision is a source of lost votes.

The scheme is also complicated for the officials. If a voter claims fraud, what is the official to do? The voter claims she voted for Jane, but both the DRE screen and the receipt show a vote for John. Should they close the polling station? On top of this, the officials are not legally allowed to see an individual voter's ballot.

VVPB addresses only a small part of the fraud problem. The paper trails themselves could be made part of a scheme for defrauding an election if a hacker tampers with the printing software. The paper can be manipulated in all the usual ways after the election.

A better option would allow people to verify their selections

THE AUTHOR

TED SELKER is the Massachusetts Institute of Technology director of the California Institute of Technology/M.I.T. voting project, which evaluates the impact of technology on the election process. A large part of his research in voting concerns inventing and testing new technology. Examples include new approaches to user interfaces and ballot design and secure electronic architectures. Selker's Context Aware Computing group at the M.I.T. Media Laboratory strives to create a world in which people's desires and intentions guide computers to help them. This work is developing environments that use sensors and artificial intelligence to form keyboardless computer scenarios.

In the Courts and in the News

In recent months, electronic voting machines have been in the news a lot, as groups file legal actions both for and against use of the machines and new problems with elections are uncovered.
—Graham P. Collins, staff editor

March—In a case brought by the American Association of Disabled Persons, a federal judge in Florida orders Duval County to have at least one machine that allows the visually impaired to vote without assistance at 20 percent of its polling places. Duval County appeals, and in April the judge stays his own ruling.

April—In Maryland, local politicians and activists from the Campaign for Verifiable Voting file suit against the Maryland Board of Elections to block the use of the state's 16,000 direct record electronic (DRE) voting machines, which do not have printers to produce paper receipts as required by state law. The move follows reports of glitches in the March 2 primary election; some voters who demanded paper ballots were given them but later learned their votes were invalidated.

April—Citing security and reliability concerns and following problems in the March 2 primary election, California's secretary of state bans the use, in the November 2004 election, of more than 14,000 DREs made by Diebold, Inc. He also conditionally decertifies 28,000 other DREs, pending steps to upgrade their security. (Some counties have their systems recertified in June.) Three counties file suit to block his order. A group of disabled voters also sues to undo the order. In addition, the California secretary of state recommends that the state's attorney general look into possible civil and criminal charges against Diebold because of what he calls "fraudulent actions by Diebold." A report accuses the company of breaking state election law by installing uncertified software on DREs in four counties and then lying about those machines.

May—In Florida, Representative Robert Wexler sues to block the use of Election Systems and Services voting technology in Broward and Miami-Dade counties.

June—The League of Women Voters, which in 2003 endorsed paperless electronic voting, drops that support. Instead it adopts a resolution to favor "secure, accurate, recountable and accessible" systems such as those with printed receipts.

June—The head of the Election Assistance Commission calls for tougher security measures for electronic voting by the November election.

July—Advocacy groups in Florida ask a Tallahassee judge to step in before the August 31 primary election and override Governor Jeb Bush's decision not to allow manual recounts in the 15 counties that have touch-screen voting machines. Also in Florida, audit records of the 2002 governor's primary and general election are reported permanently lost because of computer failures. After a few days the records are rediscovered on a disk in an adjoining room.

September—Nevada, in a primary election, will be the first to use DREs that print paper receipts statewide.

with recorded audio feedback. An audio transcript on tape or a CD has an integrity that is harder to compromise than a collection of paper receipts. Most current electronic voting machines can be set up to speak the choices to the voter while he looks at the visual interface. The tape can be read by a computer or listened to by people. Because misreads of paper are a major difficulty with all counting machines today, the tape can be better verified than paper receipts. An audio receipt is also preferable to a paper receipt because it is hard to change or erase the audio verifications without such alterations being noticed (think about the 18-minute gap on the Watergate tapes). Also, a small number of cassette tapes or CDs are easier to store and transport than thousands of paper receipts.

Other proposals for voter verification include recording the video image of the DRE and showing the ballot as it has been received by the central counting databases while the voter is in the booth. The advantage of these techniques is that they are passive—they do not require additional actions on the part of the voter.

Here is how voting might go using a well-designed audio record. Imagine you are voting on a computer. You like Abby Roosevelt, Independent. You press the touch-screen button for your choice. The name is highlighted, and the vote button on one side is replaced with an unvote button on the other side. The tab on the screen for this race shows that a selection has been made. The earphones you are wearing tell you that you have voted for "Ben Jefferson" (and these words are recorded on a backup tape).

Wait a minute! "Ben Jefferson"? You realize that you must have pressed the wrong button by mistake. You study the screen and see a prominent "cancel vote" button. You press it. "Vote for Ben Jefferson for president canceled," the computer intones onto a tape and into your ears. The screen returns to its prevote state, and this time you press more carefully and are rewarded with "Vote cast for Abby Roosevelt, Independent, for president." You go on to the Senate race.

The features just described are designed to give feedback in ways you are most adept at understanding. People are good at noticing labels moving, tabs changing, and contrast and texture changes. We have trouble doing things accurately without such feedback. The audio verification comes right at a time when the user is performing the action. Perceptual tasks (seeing movement and hearing the audio) are easier to perform than cognitive ones (reading a paper receipt and remembering all the candidates one intended to vote for). A tape or CD recording is a permanent, independent transcript of your vote.

These features are all implementable now as ballot improvements on current voting machines. Extra work would be needed to allow sight- or hearing-impaired people to verify multiple records of their ballot as well.

Some researchers are studying alternatives to DREs, in the form of Internet voting or voting using familiar devices such as the phone. Since May 2002, England has been experimenting with a number of systems intended to increase turnout. These methods include mailing in optically readable paper ballots (absentee voting), using a standard phone call and the phone's keypad, using the instant-messaging facilities on cell phones and using interactive TV that is available in English homes. Swindon Borough, for example, included more than 100,000 voters in an experiment using the Internet and telephones. A 10-digit PIN was hand-delivered to voters' homes. This PIN was used in conjunction with a password the voters had been sent separately to authorize them to vote. No fraud was detected or reported. But the effort only improved turnout by 3 percentage points (from 28 to 31 percent).

In contrast, introducing the option of absentee voting increased voter turnout by 15 percentage points—but with a downside: large-scale vote buying was reported in Manchester and Bradford. (Being able to prove whom you have voted for, such as by showing the ballot you are mailing in, enables vote buying.)

What Must Be Done

THE UNIVERSAL ADOPTION of perfect voting machines will not be happening anytime soon. But quite independent of the specific machines used, much can and should be done simply to ensure that votes are collected and accurately counted in the U.S. We must be adamant about the following improvements:

1. We must simplify the registration system. The largest loss of votes in 2000 occurred because errors in registration databases prevented people from voting. Registration databases must be properly checked, to make sure they include all eligible people who want to be registered. We must develop national standards and technology to ensure that people can register reliably but that they do not register and vote in multiple places.

2. Local election officials must understand the operation of their equipment and test its performance thoroughly when it is delivered and before each election. DREs should be tested on election day, using dummy precincts.

3. Local election officials must teach their workers using simple procedures to run the equipment and other processes. Ballot making, marking, collecting and counting all must be carefully set up to avoid error and fraud. Many voting officials inadvertently use procedures that compromise accuracy, security and integrity of ballots by, for example, turning off precinct scanning machines that check for overvotes and inspecting and "correcting" ballots.

4. Each step in the voting process must be resistant to tampering. Collecting, counting and storing of ballots must be done with documentation of who touches everything and with clear procedures for what to do with the materials at each stage. Multiple people must oversee all critical processes.

5. Each task in the voting process must be clear and accessible, have helpful feedback and allow a person to validate it. Perceptual, cognitive, motor and social capabilities of people must be taken into account when designing both machines and ballots. Ballot designs should pass usability and countability tests before being shown for final approval to the parties invested in the election.

6. The government should invest in research to develop and test secure voting technology, including DREs and Internet voting. Rushing to adopt present-day voting machines is not the best use of funds in the long term.

7. Standards of ethics must be set and enforced for all poll workers and also for voting companies regarding investments in them and donations by them or their executives.

Only when these requirements are met will we have a truly secure and accurate voting system, no matter what underlying technology is used.

MORE TO EXPLORE

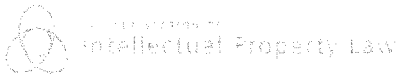
Misvotes, Undervotes and Overvotes: The 2000 Presidential Election in Florida. Alan Agresti and Bret Presnell in *Statistical Science*, Vol. 17, No. 4, pages 436–440; 2002. Available at **web.stat.ufl.edu/~presnell/Tech-Reps/election2000.pdf**

A Better Ballot Box? Rebecca Mercuri in *IEEE Spectrum*, Vol. 39, No. 10, pages 46–50; October 2002. Available at **www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html**

Security Vulnerabilities and Problems with VVPT. Ted Selker and Jon Goler. April 2004. Available at **www.vote.caltech.edu/Reports/vtp_wp13.pdf**

The Caltech/M.I.T. Voting Technology Project is at **www.vote.caltech.edu**; the project's July 2004 report with recommendations for the 2004 presidential election is at **www.vote.caltech.edu/Reports/EAC.pdf**

The U.S. Election Assistance Commission Web site is at **www.eac.gov**



An Overview of "Open Source" Software Licenses

A REPORT OF
THE SOFTWARE LICENSING COMMITTEE OF
THE AMERICAN BAR ASSOCIATION?S
INTELLECTUAL PROPERTY SECTION

The Internet?s growth during the past few years has profoundly affected the way software is licensed and distributed. One of the most important changes that has occurred during this period is the emergence of so-called "open source" licensing. The term "open source" commonly refers to a software program or set of software technologies that are made widely available by an individual or group in source code form for use, modification and redistribution under a license agreement having very few restrictions. The precursors of today?s open source licenses have existed since the early 1980s, but only in recent years have been commonly used in connection with large-scale commercial-quality software projects in recent years. The Internet is partially responsible for the increased popularity of open source projects and the open source-licensing model, because it has helped make them more cost effective and efficient for programmers to collaborate on development projects and distribute software among themselves and to customers.

For the most part, the developer community and computer trade press have focused on open source licensing?s many attractive features, such as easy access to source code and the broad community of developers, both of which contribute to the technology pool. The legal downside of the open source phenomenon has received less attention.

This paper?s purpose is to flag some of the legal issues in an effort to provide a resource for software licensing lawyers who are requested to counsel their clients on the positive and negative aspects of these licenses. Despite the many advantages of open source software licenses, there are reasons why lawyers must be cautious about recommending open source to their clients for inclusion in commercial software products.

A Brief History of Open Source Projects and Licenses

The open source software movement traces its history to the formation of the Free Software Foundation ("FSF") in 1983. The FSF was formed with the goal of creating a free version of the UNIX operating system. The FSF released a series of programs in source code form under

"GNU" name ("GNU" is an irreverent acronym that stands for Gnu?s Not Unix). The GNU project did not actually result in a free version of UNIX, but did result in the creation of some popular tools for UNIX programmers, including the GNU C compiler and text editor. It also set the stage for even more ambitious free software development projects in the 1990s.

The license agreement that accompanied the GNU software -- known as the General Public License ("GPL") or "copyleft" license -- was revolutionary for its time. It is written in a non-legalistic style with a breezy preamble and statement of purpose. The GPL gives licensees broad rights to sell, copy and modify licensed programs, so long as licensees grant to downstream licensees the same rights to sell, copy and modify the modifications to the original program. Licensees are also required to make their changes available in source code form.

For many years, the FSF filled a relatively small niche in a large and growing market for proprietary products from large companies. Many UNIX programmers used -- and continue to use -- the GNU C compiler and debugger from the FSF to create new programs targeting variants of the UNIX operating system offered by companies like IBM, Hewlett-Packard and Sun.

With the Internet?s rise in the 1990s, there has been renewed interest in free software and a shift in development resources from esoteric development tools to products and technologies having a broader commercial appeal. In 1998, a group associated with free software introduced the term "open source" to emphasize a break with the pro-hacker, anti-business past associated with GNU and other free software projects and to place a new emphasis in the community on the possibilities of extending the free software model to the commercial world. These new "open source" projects would exist in the mainstream of the commercial software market and include operating systems, such as Linux, the Apache web server, and the Mozilla browser.

What Does "Open Source" Mean Today?

The meaning of "open source" is very much in flux. According to opensource.org, an oversight organization for the open source movement, theterm "open source" doesn't just mean that licensees have access to the source code. The distribution terms of open-source software must comply with the following criteria:

1. Free Redistribution. The license may not restrict any party from selling or giving away the software as a component or an aggregate software distribution containing several programs from several sources. The license may not require a royalty or other fee for such sale.

2. Source Code. The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost -- preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

3. Derived Works. The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software

4. Integrity of The Author's Source Code. The license may restrict source-code from being distributed in modified form *only* if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

5. No Discrimination Against Persons or Groups. The license must not discriminate against any person or group of persons.

6. No Discrimination Against Fields of Endeavor. The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

7. Distribution of License. The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

8. License Must Not Be Specific to a Product. The rights attached to the program must not depend on the program's being part of a particular software distribution. If the program is extracted from that distribution and used or distributed within the terms of the program's license, all parties to whom the program is redistributed should have the same rights as those that are granted in conjunction with the original software distribution.

9. License Must Not Contaminate Other Software. The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

Source: www.opensource.org

As the open source movement has gained credibility in the marketplace, however, the term has been applied to many projects that do not fit within the foregoing parameters. For instance, Sun Microsystems has introduced a "Community Source License Agreement" that is an attempt to capture some of the spirit and momentum behind open source initiatives, but contains significant restrictions that make it substantially different from the "classic" open source licenses such as the GPL and BSD-style licenses. The Sun license in some instances requires the licensee to pay Sun a fee; it also contains restrictions on modifications that do not pass a large set of conformance tests, and purports to treat the source code as "confidential information," even though it is available for download from the Internet.

The application of the term "open source" to projects licensed under proprietary models, such as the Sun Community Source License, could help lead to reducing the term "open source" to a marketing gimmick and to confusing developers about the rights associated with various programs available under the "open source" banner. Software developers must ensure their lawyers have an opportunity to review the license agreements associated with "open source" programs before they download and use these programs in their own projects, and that their lawyers carefully review the licenses that accompany programs billed as "open source" software to ensure the licensing and other contractual restrictions are consistent with the expectations, goals and risk tolerances of individual clients.

Benefits of Open Source

There are many reasons why the "open source" model has been successful and popular with developers, including the following:

- Access to Source Code. Documentation for commercial software products is notoriously skimpy on detail and often out-of-date. This is frustrating for developers who try to write software programs that are designed to interoperate with or target other programs. The best documentation for a program is

the source code itself. Having access to source code enables the developer to understand the program at a deep level and to debug and optimize his or her own program at a level of efficiency and skill that is often not possible with programs available only in binary form.

- Community. Having a common source code pool and the tools provided by the Internet creates an opportunity for extensive and speedy collaboration on development projects.
- Cost. Most programs distributed as "open source" are free. Obviously, this is a compelling alternative to programs that cost money if the free program is equally feature rich and meets requisite performance parameters.
- Broad Rights. The broad license grant, which allows licensees to use, modify and redistribute open source programs, is a major advantage of the typical open source license. Typical commercial software products are distributed only in binary form and may not be modified. Often the documentation associated with commercial programs is not detailed enough to permit some kinds of "value added" programming that is possible for developers who have direct access to source code.

Legal and Other Risks Associated with Open Source

Along with the many benefits of open source, however, come a number of risks. Perhaps the most obvious risk is potential liability for intellectual property infringement. The typical open source project is a grass-roots effort that contains contributions from many people. This method of development can be worrisome from an intellectual property standpoint because it creates multiple opportunities for contributors to introduce infringing code and makes it almost impossible to audit the entire code base. The risks of this development process are largely borne by the licensees. Contributors do not vouch for the cleanliness of the code they contribute to the project; in fact, the opposite is true -- the standard open source license is designed to be very protective of the contributor. The typical license form does not include any intellectual property representations, warranties or indemnities in favor of the licensee; it contains a broad disclaimer of all warranties that benefits the licensor/contributors.

Even if such representations and warranties or indemnity obligations existed in open source license agreements, it would be difficult if not impossible to recover against the licensor for having licensed infringing code. Many of the most prominent open source projects appear to be owned by thinly-capitalized non-profit entities that do not have the financial wherewithal in most cases to answer for a massive intellectual property infringement suit.

The shifting of all risk for intellectual property infringement to the licensee is somewhat atypical for the commercial software world. Most for-profit software companies would require some level of contractual assurances from a licensor of software technology that such technology does not infringe intellectual property rights. By receiving such contractual assurances, the licensee shifts some or all of the risk of an intellectual property lawsuit onto the licensor, assuming of course the licensor?s capability to honor its obligations.

Open source licenses also do not contain the kinds of representations and warranties of quality or fitness for a particular purpose that commercial software vendors sometimes negotiate into agreements among themselves. Again, the process of developing open source software can contribute to problems in this area. Some open source software projects, such as the Linux initiative, have one or more stewards who monitor code quality and track bugs. Other initiatives, however, are really more the product of weekend and after-hours hobbyists and do not enjoy the

same code quality and rigorous testing protocol. Without contractual commitments of quality or fitness, the licensee must accept the risk that the software contains fatal errors, viruses or other problems that may have downstream financial consequences.

Companies looking to build a business on open source software also need to consider the problems associated with creating derivative works. Some open source license forms, such as the GPL, require licensees to provide free copies of their derivative works in source code form for others to use, modify and redistribute in accordance with the terms of the license agreement for the unmodified program. This licensing term is advantageous for the free software community because it ensures that no for-profit company can "hijack" the code base from the community. On the other hand, this licensing term makes it very difficult for companies in the commercial software business to use such open source software as a foundation for a business. These companies must be concerned that their "value added" programs might some day be viewed as "derivative works" and need to be made available to the world in source code form for free.

While the copyright attribution and notice requirements in open source licenses are relatively innocuous as compared to the issues outlined above, they nevertheless can become burdensome for the commercial software vendor. Some open source projects have multiple contributors and modules that have been created under various licensing forms. According to the terms of most open source licenses, the licensee must give each of these contributors full copyright attribution and reproduce the entire text of the license agreements for the open source code included in the product. These notices and licenses can clutter up documentation files and confuse end user customers.

Conclusion

To state the obvious, open source software offers opportunities and disadvantages. The opportunities include having a vast pool of software talent with access to, and the ability to improve upon, open source software; and the ability to access and utilize software that could be of great use but whose acquisition might otherwise have been cost prohibitive.

The disadvantages include the risk of utilizing software that infringes intellectual property rights, and that may have problems not readily apparent. The terms of various open source licenses may pose other inherent problems that may not be apparent to those not skilled in the legal nuances of licenses.

Other Resources

Specific Licenses:

Traditional open source licenses

GNU GPL (copyleft)

Library GPL

MIT X Window license

BSD Style license

Commercial "open source" style licenses

Netscape Public License -- Mozilla

Sun Community Source

IBM Jikes

Opensource.org

Debian.org

Apache.org

Articles:

"Opening Up to Open Source", Shawn W. Potter, 6 Rich. J.L. & Tech. 24 (Spring 2000)

"How Copyleft Uses License Rights to Succeed in the Open Source Software Revolution and the Implications for Article 2B", Robert W. Gomulkiewicz, 36 Hous. L. Rev 179 (Spring 1999)

This page was printed from: http://www.abanet.org/intelprop/opensource.html

Close Window

© 2007. American Bar Association. All Rights Reserved. ABA Privacy Statement