

Statement

Lillie Coney

Senior Policy Analyst
The Electronic Privacy Information Center (EPIC)

Before the
U.S. Election Assistance Commission
Technical Guidelines Development Committee

Hearing on Human Factors and Privacy

September 22, 2004
Gaithersburg, Maryland

I would like to thank the U.S. Election Assistance Commission's Technical Guidelines Development Committee for the opportunity to offer testimony before you today as you consider the subject of human factors and privacy. My name is Lillie Coney, and I am the Senior Policy Analyst at the Electronic Privacy Information Center (EPIC) based in Washington, DC. EPIC is a public interest research center established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. One of my roles at EPIC is to coordinate the activities of the National Committee for Voting Integrity (NCVI). Dr. Peter Neumann, Principal Scientist at the SRI International Computer Science Laboratory chairs NCVI. The committee was established to promote voter-verified balloting and to preserve privacy protections for elections in the United States.

Dr. Neumann expressed it best when he said, "Elections require an end-to-end concern for a wide variety of integrity requirements, beginning with the registration process and ballot construction, and continuing through vote tabulation and reporting."¹ Many of these aspects of public elections have been discussed in previous panels. Therefore, I will focus my comments today on the importance of election administration to meet the challenge of creating a sense of privacy in a polling place, the impact of electronic voting technology on privacy, and the contributions that poll workers may make to voter privacy and trust.

The laws establishing the right of citizens to participate in the public discourse associated with the act of voting have been primarily within the jurisdiction of state governments. This has resulted in a system of elections that is as diverse as it is complex, which has under certain conditions or implementation schemes frustrated the privacy of voters.² The delicate balance between the state's right to ensure that intimidation and election fraud are not present in public elections and the voter's right to privacy have resulted in the development of the secret ballot and restricted zones around voting compartments.³ Because of the documented

¹ Peter Neumann, "Statements of Support for the LCCR/Brennan Center/ Report, available at http://www.civilrights.org/issues/voting/lccr_brennan_support.pdf, June 29, 2004

² Associated Press. "Widow with Visible Vote Gets no Help," Los Angeles Times, March 12, 1992 at A15.

³ *Burson v. Freeman*, 504 U.S. 191, 207-208 (1992).

history of voter intimidation, coercion, and fraud associated with third party knowledge of how individual voters cast their ballots, it is important not to underestimate the importance of voter privacy. No community is immune to the effects of voter manipulation, but some communities are more vulnerable than others—for example those of minority, new immigrant, poor, or those in situations that allowed the unchecked political influence of a major employer to exercise economic power to affect the outcome of an election.

Living between the myth and reality—modern election systems struggle to meet the lofty expectations of Americans who view our system of government as superior to other systems of government—including other forms of democracy. Some argue that the application of technology will be the medicine that will cure the body politic of flawed elections. Others argue that the solution is found in the people who perform election administration. The truth is found in both views with two additional elements—transparency and oversight.

The Secret Ballot

Federal and state courts and legislatures have historically taken measures to protect the right of voters to vote their conscience without fear of retaliation. United States law requires that “All votes for Representatives in Congress must be by written or printed ballot, or voting machine, the use of which has been duly authorized by the State law; and all votes received or recorded contrary to this section shall be of no effect.”⁴ The statute defines “ballot” in election provisions to mean a “method which will insure, so far as possible, secrecy and integrity of popular vote,” and interprets the Congressional requirement that elections be conducted by written or printed ballots or by machine to include the notion that ballots must be secret.

As further support for the requirement of secret ballots, the statute cites *Johnson v. Clark*, 25 F. Supp. 285 (DC Tex. 1938). In *Johnson*, the District Court for the Northern District of Texas emphasized the “secrecy and integrity” of votes. “The word ‘ballot,’ in an election provision, means a method which will insure, so far as is possible, the secrecy and integrity of the popular vote.” *Id.* at 286. Other courts have also found that the concept of secrecy and privacy is inherent in the meaning of ballots. Other courts have ruled that this case clearly refers to ballot secrecy. In *Brisbin v. Cleary*, the Supreme Court of Minnesota interpreted voting by ballot to mean:

a mode of designating an elector’s choice of a person for an office by the deposit of a ticket, bearing the name of such person, in a receptacle provided for the purpose, in such a way as to secure to the elector the privilege of complete and inviolable secrecy in regard to the person voted for. This privilege of secrecy may properly be regarded as the distinguishing feature of ballot voting, as compared with open voting, as, for instance, voting *viva voce*. The object of the privilege is the independence of the voter.

26 Minn. 107, 108-09 (1879).

⁴ 2 USCS § 9 (2003), “Voting for Representatives”
EPIC/NCVI Statement

The U.S. Supreme Court has also recognized in dicta that the right to vote privately via secret ballots is an essential component of meaningful participation in the democratic process. In *Buckley v. Valeo*, the Court argued that, “Secrecy, like privacy, is not per se criminal. On the contrary, secrecy and privacy as to political preferences and convictions are fundamental in a free society. For example, one of the great political reforms was the advent of the secret ballot as a universal practice.” 424 U.S. 1, 237 (1976) (Burger, C.J., dissenting). In *Burson v. Freeman*, the Court found that “the very purpose of the secret ballot is to protect the individual’s right to cast a vote without explaining to anyone for whom, or for what reason, the vote is cast.” 504 U.S. 191, 206 (1992), quoting *Rogers v. Lodge*, 458 U.S. 613, 647 n.30 (1982) (Stevens, J., dissenting).

In *McIntyre v. Ohio*, the U.S. Supreme Court outlined the importance of the development of the secret ballot as a means of ensuring the integrity of elections.

In sum, an examination of the history of election regulation in this country reveals a persistent battle against two evils: voter intimidation and election fraud. After an unsuccessful experiment with an unofficial ballot system, all 50 States, together with numerous other Western democracies, settled on the same solution: a secret ballot secured in part by a restricted zone around the voting compartments. We find that this widespread and time-tested consensus demonstrates that some restricted zone is necessary in order to serve the States' compelling interests in preventing voter intimidation and election fraud.

Thus, the concept of voting cannot be separated from the concept of privacy, for the latter gives meaning to the former. Any legislation that would impact the voting process must always honor this marriage of privacy and integrity as central components of voting ballots. If steps are taken to undermine the secret ballot, *i.e.*, by linking a voter’s identity to his vote, then by extension the integrity of the election itself is compromised, because this opens the door to the potential for coercive tactics to influence how individuals vote.⁵

Electronic Voting Technology and Privacy

Elections in the United States may be best paraphrased by a proverb penned by Robert Burns, the eighteenth-century Scottish poet: “The best-laid schemes of mice and men...” It is no secret that the first Tuesday after the first Monday in November is Election Day. On November 2, 2004, millions of dollars, thousands of work hours, and tens of thousands of workers must be devoted to implementing a process born in the eighteenth century using twenty-first century means. In 2000, the focus was on Florida, but the problems in that state were repeated in many others. That presidential year was like any other except for one fact—the deciding margin of victory was only 537 votes. This number is dwarfed by the number of voters disenfranchised according to the CalTech MIT Study “Voting: What Is What Could Be,” which records that between 4 and 6 million votes were lost in the 2000 election.⁶ The study attributed the loss to problems with voter registration or polling place practices and problems with ballots. As a

⁵ *McIntyre v. Ohio*, U.S. Supreme Court, 514 U.S. 334, 343 (1995).

⁶ David Baltimore and Charles M. Vest, “Voting: What Is and What Could Be”, CalTech/MIT Voting Technology Project, July 2001

consequence, voters received a rude introduction to the reality of elections in the United States—not every vote cast was counted.

As a result, Congress passed the Help America Vote Act of 2002,⁷ in response to the breakdown in vote tabulation during Florida’s recount process conducted at the conclusion of the 2000 presidential election. The Florida debacle illustrated numerous problems in our election process and prompted an interest in using computing technology to solve these problems. HAVA expands the federal government's role in regulating voter registration and election processes, and it provides funds to states to upgrade their election systems. States may use the funds to replace lever or punchcard election systems with new electronic systems, to pay for election official training, to make voting locations handicapped accessible, or for other voting related expenses. Under HAVA, states retain control of the election process, but they must meet minimum standards set forth in HAVA.⁸

HAVA was generally popular among members of Congress, yet received some criticism because it required more stringent voter identification procedures. HAVA passed 92 to 2 in the Senate and 357 to 48 in the House with bi-partisan support. *Id.* Dissenters objected to HAVA because it required voters to provide either a state driver's license number or the last four digits of their Social Security Number (SSN) if they did not have driver's licenses.⁹ HAVA also required election officials to verify voters’ identification with administrative agencies (*i.e.*, comparing driver's licenses with local Departments of Motor Vehicles and SSNs with the Social Security Administration.)¹⁰ Dissenters feared that the new requirements would “raise hurdles to registration and voting by poor people and members of minority groups, especially Hispanics.”¹¹ In particular, Senator Hillary Rodham Clinton remarked that HAVA “would probably ‘repress voter participation’ by recently naturalized American citizens, homeless people and millions of New Yorkers who have no driver's license.” *Id.* Supporters of the stricter identification requirements countered that the measures were important because “illegal votes dilute the value of legally cast votes.” *Id.* According to Senator Bond of Missouri, “If your vote is canceled by the vote of a dog or a dead person, it's as if you did not have a right to vote.” *Id.*

While attempting to strengthen the integrity of the electoral process by requiring stronger voter identification requirements, HAVA did little to address the potential problems of skewed election outcomes if the electronic voting machines are faulty or rigged. David Dill, a professor of Computer Science at Stanford University, as well as a member of the National Committee for

⁷ Pub. Law Number 107-252 (Oct. 29, 2002)

⁸ Robert Pear, *The 2002 Campaign: Ballot Overhaul; Congress Passes Bill to Clean Up Election System*, *New York Times*, Oct. 16, 2002, at A1 [hereinafter *New York Times*].

⁹ “In general --Except as provided in clause (ii), notwithstanding any other provision of law, an application for voter registration for an election for Federal office may not be accepted or processed by a State unless the application includes--(I) in the case of an applicant who has been issued a current and valid driver's license, the applicant's driver's license number; or (II) in the case of any other applicant (other than an applicant to whom clause (ii) applies), the last 4 digits of the applicant's social security number.” Pub. L. No. 107-252, § 303(a)(5).

¹⁰ “Sharing information in databases.--The chief State election official and the official responsible for the State motor vehicle authority of a State shall enter into an agreement to match information in the database of the statewide voter registration system with information in the database of the motor vehicle authority to the extent required to enable each such official to verify the accuracy of the information provided on applications for voter registration. (ii) Agreements with commissioner of social security.--The official responsible for the State motor vehicle authority shall enter into an agreement with the Commissioner of Social Security under section 205(r)(8) of the Social Security Act (as added by subparagraph (C)).” P.L. 107-252, § 303(a)(5)(B)(i).

¹¹ EPIC, Comments to SSA on the Use of SSN for Voting, available at http://www.epic.org/privacy/ssn/voter_reg_comments.pdf, September 3, 2004

Voting Integrity, has stated that the use of electronic voting machines raises significant integrity and privacy issues that must be resolved to ensure the integrity of any election. Current electronic voting machines “pose an unacceptable risk that errors or deliberate election-rigging will go undetected, since they do not provide a way for the voters to verify independently that the machine correctly records and counts the votes they have cast. Moreover, if problems are detected after an election, there is no way to determine the correct outcome of the election short of a revote.”¹² According to Dill, electronic voting machines are particularly vulnerable to election fraud stemming from undetectable hacking attacks, subversive programming, and accidents.

“Computer scientists, as well as voters, are upset by paperless direct recording electronic (DRE) voting systems because we know that even a beginning programmer can write code that displays votes one way on a screen, records them another way, and tallies them yet another way. This can happen for a variety of reasons, including software and hardware errors, or ‘hacks’ installed into the voting machines. These problems can occur even when voting machines have been thoroughly inspected and tested. DRE systems experienced a number of problems already in the 2002 elections, and we see this only as the tip of the iceberg.”¹³

According to unscientific exit interviews of voters the reaction to DRE voting technology was positive. Voters’ comments regarding their experience with DRE voting machines are reported as being “great,” “very easy,” and “fast.”¹⁴ The sad truth is that the voter is the last one to recognize problems associated with voting technology. The controversy over the Florida 2000 presidential election may have come as a shock to the average voter, but it was a well-known problem among elections administrators and equipment manufacturers. The reality that not all votes were accurately recorded or counted in the typical local, state, or national election using punch card, optical scan, and DRE voting technology. What is most disturbing is that this fact may not have worried election officials very much. They could comfort themselves by saying that the votes not counted would not have changed the outcome of an election, and if it did most people would never know.

With the implementation of new voting technology, voters of all descriptions have had a multitude of experiences in recent elections. In an election held in Louisiana on Saturday, September 18, 2004, it was reported that 59 precincts did not have voting machines when polls opened at 6:00 AM.¹⁵ Unfortunately, there is no uniform mechanism for collecting the voters’ feedback on their Election Day experiences. The body of evidence is growing that voting on DRE unauditible paperless voting technology presents hazards for votes being counted as cast by voters, it is important to address these concerns. However, we must not ignore the potential

¹² David L. Dill, *et al.*, *Understanding the Problem*, VerifiedVoting.org, (2003), <http://www.verifiedvoting.org/theproblem.asp>.

¹³ Id

¹⁴ McCaffrey, Raymond and Barr, Cameron W. “Debut of New Technology Gets Mostly High Marks” *The Washington Post*. Found at: <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A24780-2004Mar2¬Found=true> March 3, 2004; Page B04

¹⁵ Doug Simpson, “Voting machines missing on Election Day in New Orleans,” available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/news/archive/2004/09/18/politics1059EDT0503.DTL>, San Francisco Gate, September 18, 2004.

threats to privacy while investigating the benefits or deterrents presented. Application of DRE paperless voting technology in US public elections address some issues of voter privacy while potentially creating others.¹⁶ Dr. Doug Jones, of the University of Iowa's Computer Science Department and a member of the National Committee for Voting Integrity, advises that DREs should separate the timestamp on the cast ballot event from the actual record of the cast ballot.

The typical scheme for avoiding exposure of how people voted when using DREs is to use a pseudorandom number generator to store "ballots" at random in the electronic "ballot box. The trouble, according to Dr. Jones, is some vendors may use a constant seed for this generator, so you could trivially determine the order of cast ballots. Others may seed the generator better, but if you have 100 ballots in pseudorandom locations in a ballot box with 1000 entries, and if the pseudorandom number generator is known, it may be a trivial matter to recover the seed by knowing which slots were used.

Dr. Jones recommends that, "It would be beneficial to privacy if DRE machines broke up the e-ballots so that the different parts, signifying votes in different races on the ballot, are stored independently. As a result, it would not be possible to sign a ballot using a pre-arranged pattern of votes in minor offices such as judicial retention races or by using a pre-arranged write-in vote in some office."

The only voting technologies that prevent this particular form of ballot signature are lever voting machines and the use of a separate ballot for each office, as some Swiss cantons do—they print the ballots on perforated paper, and before counting, separate the ballot sections into sub-ballots—leaving one section for each race.

What pseudorandom number generator used by DRE voting equipment vendors is not known, nor is it known how they are seeding it, since the source code remains proprietary, even if the seed is now changed for each election. This is not sufficient to guarantee ballot secrecy unless they have also changed to a cryptographically secure pseudorandom number generator or injected additional sources of randomness into their ballot storage algorithm.

If this has not been done, it would be a trivial matter for someone with the right computer skills to recover the seed that was used if only a small number of ballots are distributed by this generator over the slots in a much larger ballot box. For example, if there are 100 ballots in a ballot box with 1000 slots, there are well over 4 billion possible arrangements, so if a 32-bit seed is used for the pseudorandom number generator is used, the actual arrangement of ballots in ballot-box slots will uniquely identify the seed, allowing the exact order of those ballots to be inferred, and the actual votes of individual voters to be made known.

It is possible to enhance ballot secrecy if all voting machines in the same county for the same election use a different pseudo random number generator to produce different settings for distributing e-ballots.

¹⁶ <http://www.epic.org/privacy/voting/crsreport.pdf>
EPIC/NCVI Statement

The greatest privacy benefits of DRE voting machines accrue to those who are: visually disabled, language minorities, or have literacy challenges. Critics of paperless DRE voting technology acknowledge the apparent usability benefits to some voters, but point to a critical vulnerability in their design.¹⁷ Another privacy concern is presented by the implementation of the voter interface, which on some machines is done at nearly a 75-80-degree angle to the horizontal. Current machine set up in polling locations requires that the machines be in full view of the poll workers. This is done in such a manner that the display screen is exposed to those present in the polling location, including other voters. If the restricted space around DRE voting machines is too small, this would also threaten voter privacy.¹⁸

In addition to these concerns, the suggestion of applying wireless access technology to voting machines may also present privacy challenges. If misapplied, wireless access that allows remote activation could allow observation of activity on a number of voting units inside of a polling location by someone on the outside of the facility with the appropriate technology and skills. Caution should be taken when considering the implications of using wireless technology with voting systems.

Finally, the lack of a clear definition of rights for voters using DRE paperless voting technology presents an interesting dilemma. The transactions associated with voting unlike other exchanges in society, require privacy for individual voters and transparency of the overall voting system.¹⁹ The conundrum presented by paperless DRE voting technology further complicates this transaction of voter choice and privacy in a populous self-governing matrix of nearly 200 million potential participants by not producing a physical audit instrument that is verified by each voter at his or her choice. It appears to be a daunting challenge, which will require strong Federal support for research and development as new generations of voting technology emerge.

Poll Workers and Voter Privacy

According to the CalTech MIT Study “Voting: What Is What Could Be,” between 4 and 6 million votes were lost in the 2000 election.²⁰ The study attributed the loss to problems with voter registration or polling place practices and problems with ballots. The problems that I would like to focus the committee’s attention on are those associated with polling place practices.

Elections systems rely on voluntary participation of poll workers and voters. The major challenge of election systems is to create ease of use in a process that is done very infrequently. At most the greatest voter participation is seen during presidential election years, which occur once every four years. Recent reports of poll workers struggling to deal with malfunctioning

¹⁷ National Committee for Voting Integrity. Hearing Statement to the U.S. Election Assistance Commission. “Use, Security, and Reliability of Electronic Voting Systems”. 5 May 2004
http://www.votingintegrity.org/Testimony/EAC_Hearing5_5_04.html

¹⁸ Marcalus, Annamarie. “Mixed Reviews on Voting Electronically. Los Angeles Times, Metro; Editorial Pages Desk; Part B; Page 70. 6 March 2004.

¹⁹ Federal Reserve Electronic Funds Transfer Regulation E: <http://www.federalreserve.gov/regulations/default.htm#e>

²⁰ David Baltimore and Charles M. Vest, “Voting: What Is and What Could Be”, CalTech/MIT Voting Technology Project, July 2001

voting technology is not new to paperless DRE voting machines. In the Florida 2000 presidential election poll workers did not take malfunctioning punchcard voting machines out of service. It was reported that “20 [punchcard voting] machines in two Miami-Dade County precincts with the highest rate of discarded punchcard ballots did not show votes for at least some candidates during a test-vote minutes before polls opened on Nov 7.”²¹

Poll workers provide the human judgment used in a gatekeeper function to determine who may vote in public elections. There is very little if any due process accorded to voters who are judged to be invalid. Unfortunately, the experience for voters who are in the “out group” — minorities, new citizens, language minorities, and disabled voters — are most at risk of being disenfranchised. Those voters not identified with by poll workers often find the hurdles to voting are much higher and problematic. For example, in the State of Florida voters erroneously included on a list of felons, who are prevented by state law to vote, were predominately minority.

The subjective nature of the polling operation meant that some poll workers were able to recognize the errors on the list and allowed voters to vote, while others could or would not allow these individuals to vote.²² As little as possible should rely upon the subjective judgment of poll workers, as gatekeepers to the ballot box, but the focus should be on facilitating participation in the election process.

In a 2004 report on the 2003 elections in New York City, produced by the Asian American Legal Defense and Education Fund, it is reported that minority language speakers were subjected to poll workers improperly demanding identification, were rude, hostile, or made disparaging remarks about language assistance. In addition, translation signs and materials were often hidden or unavailable to voters. Some poll workers were reportedly unaware of their responsibilities or improperly refused to make language assistance available to voters.²³

Election observers placed in polling locations to monitor the election can present another problem for poll workers and voter privacy.²⁴

Most of the problems mentioned above could be addressed by adequate training of poll workers and a better screening process, as well as an affidavit requirement for poll observers that provides adequate instruction regarding their conduct inside voting locations during elections.

Poll workers should be selected for their ability to meet the requirements of the positions they are intended to fill. Monetary incentives may be a means of increasing the numbers of those willing to work at polling locations on Election Day.

An adaptation of the jury pool system currently used to satisfy the legal requirements of jury trials, that relies upon voter registration lists could be modified for a new poll worker pool

²¹ Andrea Robinson, “Machines Didn’t Pass Polling Test But All Were in Use on Election Day,” The Miami Herald, December 22, 2000. Page 1A.

²² “Use of Faulty Felon List is Seen as More Ammunition Against Fla.” The Philadelphia Inquirer, December 7, 2000, Page A27

²³ Asian American Legal Defense and Education Fund, “Asian American Access to Democracy in the 2003 Elections in NYC”, May 2004

²⁴ “The Long Shadow of Jim Crow: Voter Intimidation and Suppression in America Today,” People for the American Way and NAACP, September 2004.

program. Those participating in any poll worker pool will receive monetary compensation for two days, which should include one-day of training and Election Day. In addition, poll workers should receive three years of exemption from both jury service and poll duty. As an incentive, those who volunteer could receive five years of exemption from jury service or poll duty. Employers should be encouraged to pay employees their regular wage, when they are absent due to service as poll workers.

Another means of increasing voluntary poll worker participation may be an effective public relations campaign to increase the desire of registered voters to work at polling places on Election Day. Recently, Oprah Winfrey served on jury duty and the media coverage of that decision was positive.²⁵ Taking a similar approach to recruit athletes, musicians, actors, and others to enlist them as Election Day workers can be a great motivating tool for election worker recruitment. The public awareness campaign theme could be, "You never know who you might see working at the polls on Election Day." An added benefit may also be higher voter participation by younger voters. A pilot project would be effective in testing out ways to improve the response to the community need of poll workers to service in local elections.

Conclusion

Overly aggressive investigations of charges of voter fraud pose an additional threat to voter privacy and secrecy of ballots.²⁶ Recent reports of a Florida Department of Law Enforcement investigation that involved state troopers going to the homes of elderly black voters in Orlando to investigate their decision to vote absentee is disturbing.²⁷ Coupled with voter suppression attempts by those seeking to diminish voter participation among a targeted group also present problems to election administration and the democratic process.²⁸

In closing, it is vital that the secrecy of the ballot be extended to include men and women of the armed forces. The recent proposals made by some state election officials to use third parties agents to allow voting by any combination of scanners, e-mail, and/or fax for these individuals are particularly troubling to privacy advocates.²⁹ In the case of Missouri all three of these methods are employed for the military overseas voting program. In addition, those citizens living abroad who would like to vote should have every opportunity to do so and have that vote counted.³⁰ Every effort should be made to expedite the delivery of absentee ballot applications, wherever they are requested, which could include fax or e-mail of PDF documents, but the process of receiving voted ballots should be facilitated by special express mail designation to the state election offices. Anything less cheats these citizens of their rights to a secret ballot.

Thank you.

²⁵ Robert J. Grey, Jr., "Reinvigorating the jury system; Editorial, Chicago Sun-Times, August 22, 2004

²⁶ Leadership Conference on Civil Rights, Letter to the Honorable John Ashcroft, October 25, 2002.

²⁷ Bob Herbert, "Voting While Black," New York Times, August 20, 2004

²⁸ Bob Herbert, "Protect The Vote," New York Times, September 13, 2004

²⁹ "Denying the Troops a Secret Ballot," New York Times, page 18, Section A; Column 1; September 3, 2004

³⁰ "Pentagon Restricts Overseas Voters," New York Times, September 21, 2004