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

"Machines & Software"
March 15, 2007

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 In the rush to abandon punchcard systems and other outdated equipment, whose flaws were all-too clear in the aftermath of the 2000 presidential election, Congress subsidized and state and local governments embraced and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.