Testimony of Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University

United States House of Representatives, Committee on House Administration
Subcommittee on Elections
Hearing on
Election Reform: H.R. 811
March 23, 2007

Good morning Chairwoman Lofgren, Ranking Member McCarthy, and

distinguished members of this panel. Thank you for the opportunity to testify this

morning and provide you my perspective on H.R. 811 – The Voter Confidence and

Increased Accessibility Act of 2007. As part of my research at Princeton University, I

have reviewed the security and reliability of various voting systems. This work is

informed by my many years of experience in conducting computer security research and

debating how policy should reflect the appropriate role of computing technology.

Computers clearly have a role to play in our elections, but determining their

appropriate and best use is a complex question because of both the technology and the

multifaceted voting system to which it is applied.   H.R. 811 takes up this difficult and

contentious question, taking a balanced and thoughtful approach in outlining how new

and old technologies can work together to make elections better.

We need not choose between an all-electronic voting system and an all-paper one.

Instead, we should use computers and paper together, so that each can do what it does

best, and each can compensate for the drawbacks of the other. For example, a system

that keeps both paper and electronic records can check them against each other. A hybrid system can be easier to use, more reliable, and more secure than either an all-electronic or an all-paper system.

The key to designing a good hybrid system is to ask which things computers do well, and which are better done on paper.

Computers do several things well. They report election results quickly; they can be accessible to disabled people; and they can help voters find and fix errors before the ballot is cast. Though these promises are not always met in practice, they are reason enough to give computers a role in our elections.

But one thing today's computers cannot do is provide a simple, transparent way to record and store votes.   What happens inside an electronic voting machine – indeed, inside any computer – is complicated and cannot be inspected directly by the voter. Votes are stored as records in electronic memory, but the voter cannot tell whether the votes were recorded correctly, or whether the stored votes might be lost or corrupted later.

Because electronic records lack transparency, systems that rely on them are subject to security attacks that can modify votes undetectably, as with the voting-machine virus my colleagues and I demonstrated in Diebold touch screen voting machines. Even in the absence of a security attack, problems in all-electronic systems are very hard to diagnose – witness the ongoing dispute about what caused thousands of undervotes in November's congressional election in Sarasota County, Florida.

It is difficult, even for experts, to tell what is happening inside a computer system. We cannot "just look" to see what is happening or whether the right software is installed.

Often our only recourse is to ask the system itself what it is doing – which is fine if the system is working correctly, but questionable if the system might be compromised.

For example, logic and accuracy testing of voting machines prior to an election will tell you whether the machine is working properly before the election, but if the system has been compromised by a computer virus, or if conditions change, this testing may miss problems that crop up during the election.

Our election system must be software independent, meaning that its accuracy cannot rely on the correct functioning of any software system. Thus far, computer scientists have not found a way to ensure the correctness of useful software programs. It is unclear in general whether this is even possible. Instead of pretending we are able to ensure correctness of software, we must have a system that records and counts the votes accurately even if the software malfunctions. Had such a system been in place in Sarasota County, we could have eliminated the possibility that votes were lost due to software problems – a possibility that remains open today despite the software analysis that has been done. The only practical way to achieve software independence today is to use paper ballots.

I am not alone in making this call for software independence. The Association for Computing Machinery – one of the largest, oldest and most well-respected computing organizations – has pointed out the need for independent verification in electronic voting systems[1]. Further, last year the federal body charged with developing standards for

---

[1] ACM Policy Recommendations on Electronic Voting Systems, September 2004,

3

voting systems – the Technical Guidelines Development Committee – passed a resolution[2] calling for software independence in the next version of federal standards for voting systems. This was based on the finding by the independent and well-respected National Institute of Standards and Technology, that there is currently no way to create a testing protocol that will certify that voting software is free of security and reliability problems.

By comparison, paper recordkeeping is much more transparent. A properly designed paper record conveys the voter's intent clearly, and the voter can confirm this by inspecting the paper record. (Blind voters can do this with the help of assistive technology.) Unlike a volatile electronic record, a durable paper record will not change unexpectedly.

Of course, we need to avoid poorly designed paper systems such as the punch cards used in the Florida 2000 election. Such systems are difficult for voters to inspect and suffer from problems, now well known, in determining the voter's intent. The solution is not to eliminate paper entirely, but to use a better paper record.

Looking at the strengths and weaknesses of electronic and paper-based systems, we can draw two conclusions. First, the primary record of a vote should be paper,

http://www.acm.org/usacm/Issues/EVoting.htm

[2] Resolution # 06-06: Offered by Dr. Rivest, "Software Independence of Voting Systems", http://vote.nist.gov/AdoptedResolutions12040506.pdf

because paper recording is more transparent and the paper ballot can be verified directly by the voter. Second, computers can sensibly be used for other parts of the voting process, such as entering the votes, providing a quick count (subject to auditing), and helping to reduce voter error.

H.R. 811 follows this blueprint. It requires the use of a durable, voter-verified paper ballot. Beyond this, it gives states and localities the choice of whether and how to use computers in their elections.

Different jurisdictions will use computers differently. Some may use a DRE touch screen voting system with a "ballot under glass" paper trail add-on. Some may use optical-scan ballots that are marked manually by voters and counted by electronic scanners that also collect the marked paper ballots. Some may use touch screens as ballot-marking devices that print out a paper ballot suitable for optical scanning. As long as there is a suitable paper ballot and the appropriate technical standards are met, each jurisdiction can choose among these and other alternatives.

There are different types of paper records too. Some systems store the paper records on a long roll of paper. Because they record votes in the order they were cast, these systems fail to preserve voter privacy. H.R. 811 rightly requires the paper record to preserve privacy. A better paper trail has a separate piece of paper for each voter, or uses a paper spool in "cut and drop" fashion by cutting each record off the spool (or breaking it at a perforation) after it is printed, and letting the individual records drop into a closed bin. H.R. 811 gives jurisdictions choices here too, as long as the paper records are durable, voter-verified, and privacy-preserving.

Because computers can count and tabulate ballots quickly, many jurisdictions will want to gather quick electronic counts when the polls close. Usually the electronic count will match the results that would be reported by a manual count of the paper ballots. However, because the paper ballots are the primary records, we need to make sure that the electronic count matches the paper ballots. To do otherwise – to report a result without ever consulting the primary records of voter intent – would defeat the purpose of using a voter-verified paper record. The solution is a random audit in which we count a random subset of the paper ballots and compare the result to the corresponding electronic count. If the results match, we can be confident that the electronic count is accurate enough. To have confidence in the result of the random audit, we need to audit enough precincts to be know that we are not missing problems that could significantly affect vote totals. H.R. 811 requires a suitable random audit.

Although the paper record is the primary record, there will be times when the paper record is lost or damaged. This will be very rare in a well-designed system, but it will happen once in a while. When it does happen, it makes sense to use the electronic record to backstop the failure of the paper record, but only when a suitable showing has been made with respect to the paper records kept by specified voting machines. This again is the approach taken by H.R. 811.

E-voting faces numerous challenges and is a field ripe for further research. Federal and private investments should continue to be made and new, innovative

approaches should continue to be developed. For example, fully electronic verification technologies may at some future time become a viable substitute for voter-verified paper ballots, once researchers have worked out the details necessary to deploy them in the real world accessibly and securely.   However, until the fundamental constraints of security reliability, and usability can be adequately addressed, these systems should not be certified.

Improving our elections will cost some money, but this is a bargain if it brings our elections up to the level of security, reliability, accessibility, and privacy that all citizens deserve.   Computers can make our elections more secure and more reliable; passing H.R. 811 would be an important step in realizing that promise.

Biography of Edward W. Felten

Edward W. Felten is Professor of Computer Science and Public Affairs, and Director of the Center for Information Technology Policy, at Princeton University. His research interests include computer security and privacy, Internet software, and information technology policy. He has published more than eighty papers in the research literature, and two books, and he is widely quoted in the press as an expert on security, privacy, and information technology policy. He has advised the U.S. Departments of Justice, Defense, and Homeland Security, and the Federal Trade Commission, on security-related issues. He serves on the Executive Committee of USACM, the U.S. public policy committee of ACM, the leading professional society for computer scientists. In 2003, Scientific American magazine named him to its list of fifty global leaders in science and technology.