January 26, 2007

The Chronicle of Higher Education
1255 23rd Street, N.W., Suite 700
Washington, D.C. 20037

To the Editors:

Your article "Georgia's Unusual 'Electoral College'" misses several reasons why the computing community has expressed concerns about e-voting machines and called for independent verification of votes. The article also has statements that were simply quoted without verification or critical analysis.

Although the article focuses on direct recording electronic (DREs) machines' vulnerability to hacking, hacker access is only one issue facing election officials. Elections can be undermined by undetected errors, unforeseen complications, or insiders seeking to commit election fraud. Some of the known problems from the November 2006 election occurred not because of hackers, but because the technology failed in unexpected ways.

The security, reliability and usability issues around these threats must be addressed responsibly. Based on decades of experience in building complex systems, experts in security and reliability have concluded that voters need a method of determining their votes independent of software to ensure the integrity of elections. Paper systems are currently the only way to provide this independent verification. ACM, our parent organization, formally adopted this position in 2004. In December 2006, National Institute of Standards and Technology (NIST) personnel reported that there is no way to write testable security requirements that will guarantee secure, reliable DRE's. They concluded that paper trails are needed for voters to verify their votes independent of the underlying software.

Your article quotes Mr. King as suggesting that adding continuous roll paper rolls onto DREs represents the best practice for paper-based independent verification. To the contrary, these solutions undermine privacy, are unreliable, and represent an ad hoc approach rather than a carefully engineered audit system. Instead of indicting paper trails, we urge further research into verification systems. We also note that robust paper audit trails are produced by existing precinct-based optical scan machines and ballot marking systems, thus providing paper-based independent voter verification. Mr. King is also quoted as contending that paper systems cannot be used by the blind, or by those

who cannot read English. In fact, several systems are available for use by the visually impaired, and ballots can be printed in other languages.

Mr. King's assertion that the Georgia machines cannot be hacked is not verifiable. His claim contradicts decades of research showing that such determinations cannot be made for significantly-sized software artifacts and numerous independent studies revealing serious security flaws in e-voting machines. Additionally, voting machine vendors have continually erected legal barriers to prevent competent, independent researchers from gaining access to their source code so that it may be critically evaluated. Rather than have closed investigations of e-voting machines with potential conflicts of interest, such as at Kennesaw State, research should be done in an open and transparent way.

The public's confidence in fair elections is crucial. Articles that fail to research and refute fallacious statements; that equate conclusions by internationally-known technology experts with statements of an undergraduate student; and that repeat pejoratives about respected professionals do a disservice to your readers and to the information technology community.

Eugene Spafford, Ph.D.
Barbara Simons, Ph.D.
On Behalf of the U.S. Public Policy Committee of the Association for Computing Machinery