Rebecca Mercuri's Electronic Voting Press Quotes

Updated 2/23/04

<-- Return to Electronic Voting Homepage

The excerpts on this page provide a newsworthy overview to the Mercuri opinion on this subject. Check out the full articles via the original http citation (some may expire) or, more easily, by clicking on the title of the article (for an archived copy). Only articles directly referencing Rebecca Mercuri's comments or work are included here, other relevant pieces can be found via the links on her Electronic Voting homepage. Citations are listed in reverse order of publication (most recent first) within the following sections:

Standards

This section features coverage of ongoing election standards efforts.

"Standardize voting, experts tell Congress," Mike Martin, UPI, May 22, 2001.

> Rebecca Mercuri, president of software consulting firm Notable Software, provided the committee a "top ten" list of problems with today's electronic balloting and tabulation systems. She insisted that a body of standards, developed by an agency such as the National Institute of Standards and Technology (NIST), is necessary to avoid a repeat of the 2000 presidential election crisis.
>
> Mercuri said the public voting process is, ironically, entrusted to a small group of individuals -- those who program, construct, and maintain voting machines.

"Computer Scientists and Political Scientists Seek to Create a Fiasco-Free Election Day," Florence Olsen, The Chronicle of Higher Education, April 20, 2001. http://chronicle.com/infotech

> Voting by secret ballot on computers and the Internet poses unique privacy and data-security problems. No solutions are in sight, but computer scientists find such challenges appealing, says Rebecca Mercuri, a visiting lecturer in computer science at Bryn Mawr College. "We like problems like that, that we can't figure out solutions to."
>
> Ms. Mercuri attracted a lot of attention after the election because of the arguments in her dissertation in computer and information science at the University of Pennsylvania -- "Electronic Vote Tabulation: Checks and Balances" -- which she defended in October,

two weeks before Election Day.

The manufacturers, she says, claim but cannot prove that their computerized systems protect both the secrecy and the integrity of votes. System logs can show whether a computer has been tampered with -- but those same logs also can be used to identify how individual citizens voted.

"It's very, very difficult to maintain system security, maintain system logs, and provide the voter with the secret ballot as required," says Mr. Craft, the Florida election-systems chief. He agrees with most of what Ms. Mercuri writes, with one exception. "She seems to be saying you shouldn't use computers to conduct elections, and I don't agree with that." ...

Ms. Mercuri favors having the Commerce Department's National Institute of Standards and Technology certify the accuracy and integrity of any computer-based voting system used in federal elections. States would permit counties to purchase only certified systems. ...

In February, faculty members on the Caltech/M.I.T. team published their preliminary data. Ms. Mercuri says the statistics confirmed what she and other computer scientists "had believed in our gut": that old-fashioned lever machines and paper ballots are the most accurate and easily understood voting technologies in use today. "People are laughing and calling me a Luddite," she says, "and here Caltech and M.I.T. come out with the same thing!"

Both of the older technologies, she says, have safeguards that are lacking in punch-card machines and touch-screen D.R.E. voting systems: Should a hand recount of votes become necessary, paper ballots make it easy. Votes cast on lever machines can't be recounted, but the machines can be inspected by opening them up to see, for instance, whether a gear has slipped or been tampered with. If problems are discovered, the counting errors are usually limited to only one or a few machines, she says. But a programming error in the D.R.E. software that creates ballots or counts votes affects not just one but every machine in the county. If a recount is needed, there are no paper ballots to serve as backups.

"The machines have [failed] and do fail," says Ms. Mercuri, who serves as an election official in Mercer County, N.J. On Election Day 2000, for example, a few major-party candidates received no votes at all in some New Jersey jurisdictions that were using new D.R.E. equipment. When election officials there raised questions, she says, the manufacturer maintained that no votes had been lost -- the explanation, it said, was that "no votes were cast for those candidates."

"America is a Patchwork of Voting Methods," Larry Lipman, Cox Washington Bureau, November 22, 2000.

Electronic systems also are subject to failure. They also count votes as a running tally and do not produce an actual ballot that can be recounted or compared to the tally given by the machine.

Rebecca Mercuri, president of Notable Software Inc. who has studied electronic voting for

a decade, said such systems can have serious flaws including errors in hardware and software that can give inaccurate results.

Optical scanning systems grew in popularity during the past decade, particularly in smaller counties. They work much like a paper ballot but can be more quickly -- and presumably accurately -- counted than ballots counted by hand. But because ballots are scanned by a machine, they must be printed with extreme precision. Circles or boxes printed one-32nd of an inch off might not be properly read, Brace said.

Mercuri noted that when circles that are not precisely filled in they may not be accurately counted by optical scanners.

Trends

Information in these articles is related to purchases and construction of new voting equipment.

"The Angler: Democratic glitch," Red Herring, July 31, 2001. http://www.redherring.com

Rebecca Mercuri of Bryn Mawr College, a noted expert in election technology, agrees. At an event at the National Press Club in January, Ms. Mercuri called the current state of election software a "Pandora's box." She continued, "Some years down the road the box will open to reveal yet another election fiasco, but this time instead of hanging chad, we will have disappearing electrons."

"Can the Swedes Swing the Net Vote?," Joe Berkofsky, TechTV News, April 11, 2001. http://www.techtv.com/news/politicsandlaw/story/0,24195,332142,00.html

"The issues with Internet voting have less to do with technology than with social problems: vote-selling, as well as coercion, not to mention voter fraud," Mercuri said Wednesday.

Already vote-selling cropped up in the 2000 election, she said, when the site VoteAuction.com offered votes to the highest bidder. While New York barred the site, it moved to an offshore address and any Net election could encourage such bartering on a much wider scale, she said.

Net elections could also encourage wider voter coercion, she said, because groups might bring computers to poor areas and stand "over their shoulder" as voters e-voted online.

Safevote's system also fails to secure against denial-of-service attacks and power outtages, both of which could hamper Net voting, she said.

"Even if Ed or someone else came up with the perfect Internet voting system, it doesn't address these other issues at all," she said.

"Debugging Democracy," Wired Magazine's "GIGAtrends: What's Next" issue, April 2001. http://www.wired.com/wired/archive/9.04

FALSE ALARM: Political machines can't be trusted: All-electronic systems and Internet

crypto fall far short of ensuring "one person, one vote." Good point, and that's why total automation isn't the goal -- experts warn that error and fraud are best minimized by human oversight at each step of the process.

WORDS TO LIVE BY: "All current and recently proposed systems are inadequate." -- Rebecca Mercuri, a Bryn Mawr College computer science professor whose court affidavit advocated hand recounts in Florida.

"Finding Profit in Chad," Joshua Kurlantzick, U.S. News & World Report, March 5, 2001. http://www.usnews.com/usnews/issue/010305/evote.htm

Yet many computer experts are not enthusiastic. "Government services online have low privacy standards, but E-voting would pose a greater privacy risk," says Rebecca Mercuri, lecturer in computer science at Bryn Mawr College. Mercuri notes that no E-voting system has been certified as complying with government security standards.

Adler acknowledges these complaints but insists VoteHere's technology is secure. "It will take time to create the familiarity with E-voting that quells concerns," he says.

No paper trail. E-voting has other drawbacks. Electronic balloting systems without printouts make it harder to check results, Mercuri says. In one infamous example, St. Petersburg, Fla., used computerized counting in a mayoral election. A tabulation mistake, caused either by computer error or by human fraud, gave 1,429 extra votes to the incumbent, who won by 1,425. Without a paper trail, mistakes could not be analyzed.

What's more, E-voting could create demographic divides. Older, less technology-literate people might be less willing to vote, warns House Majority Leader Dick Armey, one of Congress's experts on E- government. A 1999 poll found only 19 percent of Americans over 65 would support Internet voting.

Despite these concerns, E-voting appears to be a go: At a recent trade show, members of Congress cooed over new voting systems. Will the systems really be revolutionary--and profitable? "Undoubtedly," Adler says. Will they work? "They could lead to a fiasco that will make Florida look minor," says Mercuri.

"Electronic voting: convenient or inherently flawed?," IEEE Institute, February 2001.

The Internet Voting Task Force of California, USA, is one of the leaders in the movement to implement electronic voting. Such a system, which would allow greater convenience, safety and easier access for voters, is being considered in the United States, the United Kingdom and some countries in South America.

If the Task Force's gradual four-step plan were adhered to, voters would be able to cast ballots using Internet connections at their local polls, and then in time, ultimately be able to vote from other polls, libraries and even home.

But Dr. Rebecca Mercuri, an expert in the field of electronic voting who was requested by the U.S. Democratic Party Recount Committee to testify to the necessity of a Florida hand

> recount in the 2000 U.S. election, said there is an inherent problem with voter privacy in such a system.
>
> "There is no way to separate the pass code (password) from the ballot," Mercuri said. "They both transmit together, and therefore the vendor has access to the voter's password. There is also no way to audit or verify votes. Finally, there is the usual concern for hackers and viruses, as well as the potential for vote-selling."

"No E(asy) Cure," Wendy M. Grossman, Scientific American, February 2001. http://www.scientificamerican.com/2001/0201issue/0201cyber.html

> Doctored software isn't the only risk. There are also power failures, bugs, hacker attacks and uncertainty whether the software inside the voting machine is the same software that was approved by the state. In Internet voting, there's the political issue of shifting the burden of supplying and maintaining the voting infrastructure from election officials to individual voters. Not to mention the fact that not everyone has access to the Internet. Even the argument of lowered costs is specious, says Rebecca Mercuri in the November 2000 Communications of the ACM, when you compare the costs of mailing out passwords and authenticating voters with the costs of today's well-understood absentee ballots. (Mercuri, a faculty member at Bryn Mawr College, successfully defended her doctoral dissertation on the perils of electronic voting last fall; when published, it is expected by some to be one of the most comprehensive contributions to the subject.)

"The search for a new voting system," Matt Carr, The Prince George's Sentinel Newspaper, January 30, 2001.

> The voting technology solutions are challenged on both technical and social grounds by critics ranging from Rebecca Mercuri, visiting lecturer in computer science at Bryn Mawr College, and Lance Hoffman, professor, GW Department of Computer Science, to Kim Alexander, president, California Voter Foundation and Deborah Phillips, president of Voting Integrity Project. While Internet voting poses greater challenges - especially concerning privacy, voter authentication, and coercion - basic objections continue to be made to the reliability of on-site electronic voting machines.

"Rush to newfangled voting machines abates," Seth Borenstein, Detroit Free Press, January 25, 2001. http://www.freep.com/news/politics/vote25_20010125.htm (A longer version of this article also ran in the Akron Beacon Journal, January 14, 2001 as "To Build a Better Election.")

> "It's totally a people problem," said Rebecca Mercuri, president of Notable Software, a computer security consulting firm, and a lecturer at Bryn Mawr College in suburban Philadelphia.
>
> "People are looking for the quick answer, and they're looking for technology to provide the quick fix," Notable Software's Mercuri said. "What they're going to get is the quick mess."

"Let's not rush into electronic voting," Dan Gillmor, San Jose Mercury News, January 16, 2001.

http://www0.mercurycenter.com/svtech/columns/gillmor/docs/dg011701.htm

> Despite the outcry for new electronic voting systems, government officials should proceed with utmost caution in this area, argues columnist Dan Gillmor. The current energy crisis in California was a result of the impatience of that state's lawmakers in 1996. In the same way, the federal government's eagerness to mend a flawed election process could land us in a dangerous situation in another four years, Gillmor contends. Peter Neumann, principal scientist at SRI International's Computer Science Lab, testified before a California election committee, urging them to take caution. "You can't trust the software platforms on which systems are running. You can't trust the servers. You can't even be assured you're getting software from the server you think you're getting it from," he said of the inherent risks to Internet voting. Rebecca Mercuri, computer science professor at Bryn Mawr College, says that, even with non-Internet electronic voting, a paper trail is absolutely necessary. The idea that a paper process is flawed ignores the potential problems connected with electronic voting. Additionally, many of the problems experienced in previous elections were due to the lack of personnel, as election officials do not have enough resources. (Article abstract from ACM TechNews, Volume 3, Issue 153, January 17, 2001. technews@hq.acm.org)

"City to get high-tech voting machines," Jeff Gelles, Philadelphia Inquirer, January 15, 2001 (cover story). http://www.phillynews.com (Do search for: Rebecca Mercuri)

> The machines' critics say the main problem is a potential improvement they lack: an auditable paper trail that enables a voter to verify the accuracy of his or her own vote and allows a meaningful recount in a contested race.
>
> "I actually think that they should suspend [the purchase], and I am not alone in my belief," said Rebecca Mercuri, a Bryn Mawr College computer scientist whose research has focused on problems with computerized voting systems. She said Philadelphia would be better off doing nothing for the time being, or even turning to optically scanned ballots, a newer paper-ballot system that eliminates the most glaring faults of punchcards.
>
> ..."If we as a nation are looking at voting systems, and the City of Philadelphia goes and buys a new voting system, they're going to have a potentially obsolete voting system when the new standards come out," Mercuri said.
>
> ...To computer scientists such as Mercuri and Neumann, any proposal that lacks a paper trail risks putting too much faith in computer systems. Even some highly secure systems have shown themselves vulnerable to misprogramming or hacking, they say.
>
> "If we did have a way of designing a software product that was perfect, we would never have bugs, we would never have a computer crashing," Mercuri said.
>
> ...Although there is also no paper trail on Philadelphia's mechanical machines, Mercuri said the simplicity of the machines' levers, gears and counters makes tampering easy to recognize.

> By contrast, she said, electronic machines rely on complex computer code that even outside experts could have a hard time deciphering. And the code is considered proprietary, so outsiders would have limited opportunities to test it.

"City buying voting machines," Dave Davies, Philadelphia Daily News, January 5, 2001. http://dailynews.philly.com/content/daily_news/2001/01/05/local/VOTE05.htm

> Bryn Mawr College computer science professor Rebecca Mercuri has been warning against DRE voting systems since the early '90s. Her argument is simple: because votes disappear into a magic screen, there's no way to tell later if they were accurately recorded.
>
> "The voter has no way of knowing if what they pushed on the screen is what was recorded on the computer," Mercuri said in an interview. "I can program a computer to show one thing on the screen, print a different thing on a printout and record something else on a cartridge."
>
> Critics can point to few examples of electronic voting systems going haywire around the country, but they argue that's because of the inherent problem that tampering is undetectable.
>
> A recount is quick and easy, but it only confirms what the computer recorded, whether it's accurate or not.
>
> Mercuri believes the only way to make electronic systems truly auditable is for each voter to review a printed copy of his or her vote, which goes into a box, so it can be compared with the computer-recorded votes later if necessary.

"Will New High-Tech Voting Methods Put End To Florida-Style Vote Chaos?", Benjamin Kepple, Investor's Business Daily, December 14, 2000.

> A DRE machine in New Jersey failed to count votes in a local race. No one noticed until it was too late. "One of the machines was obviously not lighting up some of the votes, but the election workers said the lights had burned out," said Rebecca Mercuri, computer scientist at Bryn Mawr College. "At the end of the day, there were 0's by some of the candidates."

"Election debacle highlights debate on new voting systems," Earl Lane, Newsday, December 14, 2000.

> "I and many 12-year-olds can write a program that would print one thing on the screen and a different thing in the ballot cartridge" that records the votes in an electronic voting machine, said Rebecca Mercuri, a specialist on voting machines who teaches computer science at Bryn Mawr College in Pennsylvania.
>
> Electronic voting machines typically retain a record of a voter's selections both in a machine's hard drive and in a removable memory cartridge. The machine can print out a paper record of the data, Foster said, with the sequence of votes randomized to prevent potential identification of voters by their time of voting. But Mercuri and others argue that

such a record is not the same as individual paper ballots that can be kept for later review and manual recount if needed. She advocates adding a feature to the electronic machines: After a voter enters touch-screen selections, the machine also would produce a printout of the ballot choices, which the voter would verify and place into a secure ballot box as a backup.

"County Studies Plan for New Voting Machines," Steve Berry, Los Angeles Times, December 11, 2000. http://www.latimes.com (Do search for: Rebecca Mercuri)

Rebecca Mercuri, a computer scientist at Bryn Mawr College in Pennsylvania, said voters still need assurance that the computer accurately records the votes they cast. "A lot of people, including me, can write a program that will show one thing on the screen and send something different to the disk."

"The Risks of Touch-Screen Balloting," Henry Norr, San Francisco Chronicle, December 4, 2000.

Much more serious objections came from Peter G. Neumann, and he's certainly not someone to argue with lightly: He's principal scientist at the Computer Science Lab at SRI International in Menlo Park, chairman of the Association for Computing Machinery Committee on Computers and Public Policy and author of a book called "Computer-Related Risks," among many other distinctions. Among his areas of expertise is the problem of election security.

In essence, he argues that the challenge of ensuring the integrity of elections conducted on electronic equipment is much greater than my column suggested. In fact, he describes touch-screen systems as "disasters waiting to happen -- with enormous opportunities for fraud and accidents that are very difficult to detect and almost impossible to rectify."

Through Neumann I also heard from Rebecca Mercuri, a computer scientist who recently completed a Ph.D. dissertation on "Electronic Vote Tabulation Checks & Balances." In laying out a perspective similar to Neumann's, she focused in particular on the absence of an audit trail with electronic systems:

"It is essential to elections that there be an alternative method for independently verifying that the votes cast correspond to the totals reported. Since I (as well as many 12-year-olds) can write programs that accept one input value, record a different one and report yet another, computer systems can be no more trusted to provide their own verification than can a fox guarding the hen house."

Both Mercuri and Neumann cited the experience of New York City, which spent more than 15 years and $17 million in search of an electronic system to replace its lever machines. At one point city officials even signed a contract with Sequoia-Pacific, a well-known manufacturer of voting equipment, but canceled it after experts, including Mercuri and Neumann, pointed out problems with the system, particularly in the area of security.

In the end, the city gave up because, according to Mercuri, no vendor could satisfy the security requirements in a specification that was "not really very strict" by her standards.

> If you want to check out their arguments for yourself, go to Neumann's page, www.csl.sri.com/~neumann, scroll down to the section on Computer-Related Elections, then follow the links. For Mercuri, go to her company's site, www.notablesoftware.com, and click on Electronic Voting.

"E-voting," Laura Forlano, Gotham Gazette, December 2000. http://www.gothamgazette.com

> But it is not just an issue of expense. "I don't believe that just because a technology is old that it means that it should be thrown out," said voting security expert Rebecca Mercuri in a November 30 interview with WBAI http://www.wbai.org in New York. Mercuri recently completed her doctoral dissertation, "Electronic Vote Tabulation Checks & Balances," at the University of Pennsylvania's School of Engineering.

"Time for online voting?," John Winters, Sun Chronicle, November 25, 2000.

> [This is not the first time (nor probably the last) that I've been referred to as a Luddite (on this matter) in public. I consider it a badge of honor, but also don't intend to quote from the article here! You can read this sorry piece for yourself under the link.]

"In the Running," Doug Brown, Interactive Week, November 22, 2000. http://www.zdnet.com/intweek

> Any system connected to the Internet could get infected with hidden code that would subtly alter vote tallies, said Rebecca Mercuri, a computer scientist at Bryn Mawr College who last month successfully defended her University of Pennsylvania Ph.D. thesis, titled *Electronic Vote Tabulation Checks and Balances*.
>
> "We can only eradicate viruses after we know they are there," Mercuri said, adding that electronic voting methods of any sort are inferior to traditional voting methods because they replace paper ballots with bits and bytes. Florida, she said, has shown the importance of audit trails. In contemporary electronic systems, legitimate recounts are impossible because digital ballots are invisible and too easily corrupted.

"Computer voting: Attractive, but flawed," Seth Borenstein, Philadelphia Inquirer Washington Bureau, November 14, 2000. http://www.krwashington.com/content/krwashington/2000/11/13/elections/BC_ELN_PRESIDENT_VOTING_WA_national_political.htm

> There must be a better way, right?
>
> "All voting systems, including the new ones being proposed - the Internet and direct-entry balloting - they all have flaws," said Rebecca T. Mercuri, a computer-science professor at Bryn Mawr College who consults for the Democratic Recount Committee in Florida. "The question is, which flaws do you trade off for?"

Election 2000

Events and issues pertaining to the November 2000 election (in Florida and elsewhere) are examined.

"Big Lie: Every vote counts," Paige St. John, Tallahassee Democrat, December 17, 2000.

> But this year in Trenton, N.J., one direct entry voting computer improbably showed no votes for two local candidates' running mates.
>
> "The computerized machines are not so flawless," said Rebecca Mercuri, president of Notable Software Inc. and a professor of computer-related risks at Bryn Mawr College in Philadelphia.
>
> Mercuri argues that she believes the electronic voting machines cannot be audited, paper printouts notwithstanding.
>
> "I can teach my first-year students how to show one thing on the screen, print something else on the paper tape, and record something different on the computer disk," Mercuri said.
>
> "It's sort of scary, because a lot of places want to throw out these punch cards and switch to something really scary. People keep flinging around words like, 'If we had modern computers and new technology we should change things.' In fact, that is not the case because there really is no regulation on these types of machines. And very few municipalities have either the funding or the knowledge to assess these pieces of equipment."

"Votescam 2000 The Real Scandal Is the Voting Machines Themselves," Jonathan Vankin, New York Press, December 13, 2000. http://www.nypress.com/content.cfm?content_id=3261

> "DREs are even worse," says Rebecca Mercuri, a computer scientist at Bryn Mawr who's studied computerized elections for more than 10 years and recently finished her doctoral dissertation on that exact topic at the University of Pennsylvania. DREs leave no "audit trail" (paper trail) whatsoever, she points out. Votes are recorded directly onto a memory cartridge. There is absolutely nothing to ensure that the vote that registers on the screen is the vote that gets recorded on the cartridge, or that the vote that is recorded on the cartridge is the vote that prints out on paper.
>
> "Unless the voter sees that paper trail, how do they know?" she says. "I could teach a 12-year-old to write a program that shows one thing on the screen and another thing on the printout."
>
> While some newer election computing companies say they've figured out how to create a foolproof electronic audit trail, Mercuri dismisses such claims as "preposterous." There's no way to make sure that software is 100 percent pure. "If we could do that in computer science, we'd have the virus problem solved," she says.

"Bush seeks to halt hand count," Glen Johnson, Boston Globe, November 12, 2000.

> Problems with automated vote-counting equipment, especially the computer punch card type used in southern Florida, have been well documented, said Rebecca Mercuri, a visiting professor of computer science at Bryn Mawr College.
>
> "You will never get the same numbers," she said. "If you run thousands of these cards

through again and again, you will continue to get different numbers that are coming up.

"A Modern Democracy That Can't Count Votes," Special Report, Los Angeles Times, December 11, 2000 (cover story). http://www.latimes.com (Do search for: Rebecca Mercuri) Reprints include:
Seattle Times 12/12/00 as:
"Balloting bedlam: Count it the norm Lapses not just in Florida, but across U.S."
The Record (Northern New Jersey) 12/12/00 as:
"FROM COAST TO COAST, VOTING SYSTEMS IN NEED OF REPAIR"
Pittsburgh Post-Gazette 12/13/00 as:
"FLORIDA ELECTION BUNGLING REPEATED IN MANY STATES"
Winnipeg Free Press 12/15/00 as:
"U.S. vote system in chaos Ballots land in Denmark, Q-Tips rig vote machines"
Orlando Sentinel 12/17/00 as:
"FLORIDA IS NOT ALONE NATIONWIDE, VOTING SYSTEMS ARE OPEN TO FAILURE"

> Rebecca Mercuri, a computer scientist at Bryn Mawr College in Pennsylvania, and Curtis Gans, director of the nonpartisan Committee for the Study of the American Electorate, estimate that at least 2 million ballots did not get counted this year across the country.
>
> That would disenfranchise a city the size of Houston.

"Different votes for different folks in N.J.," Joseph Dee, Trenton Times, November 16, 2000 (cover story). http://www.nj.com/news/times/index.ssf?/news/times/11-16-2ARCFKVC.html

> Before we New Jerseyans develop a smug sense of superiority and suggest we are immune to the type of vote-counting fiasco plaguing Florida, know this: It could happen here.
>
> The technology is antiquated, but it works, says Rebecca Mercuri of Lawrence, an expert on voting machines who teaches computer science at Bryn Mawr College in Pennsylvania.

"Both machine, human needed to tally votes," Toni Locy, USA Today, November 20, 2000. http://pqasb.pqarchiver.com/USAToday/ (Do search for: Rebecca Mercuri)

> What's the most accurate way to count votes in a tight election? Is Texas Gov. George W. Bush right that it's with machines? Or is Vice President Gore correct that it's with human hand counts? Experts say that neither is exactly right. Nor exactly wrong. They say hand counts and machines are both needed to do the job right.
>
> Urosevich [a vice president of Election Systems & Software Inc. of Omaha] says machines that read punch cards are 99.9% accurate, and maybe as much as 99.999% right. In a close contest, that's not as good as it sounds. In Florida, where 6 million votes were cast, machines with 99.9% accuracy could have mistakenly rejected 6,000 votes. Machines with 99.99% could have kicked out 600. And those operating at 99.999% accuracy could have disregarded 60 ballots.
>
> "That's a significant number of votes, and in a close election, a hand count is not only

necessary, it's essential," says Rebecca Mercuri, a computer science instructor at Bryn Mawr College in Bryn Mawr, Pa.

"COUNTING THE VOTE: THE MACHINE; New Focus on Punch-Card System," Ford Fessenden, New York Times, National Desk, November 19, 2000. http://archives.nytimes.com
The New York Times Learning Network also featured a Mercuri quote in their November 20, 2000 current events activity. Access it here or at:
http://www.nytimes.com/learning/teachers/snapshot/student/20001120.html

> Rebecca Mercuri, the president of the consulting firm Notable Software and an authority on electronic voting tabulation, said: "There's such pressure to get the returns quickly. You can run the punch cards through at a high rate of speed, print out the computerized report, assume it to be correct, and get the results broadcast on the 11 o'clock news."
>
> For that speed, the machines sacrificed accuracy. "With any marginal card, the card reader says, 'I'm going to throw that out,' " Ms. Mercuri said. It does not mean that a voter did not vote a certain way, just that the machine cannot be sure, whether because of chad -- as the paper punch squares are known -- or some other technical issue. "It's a false negative and it needs to be relooked at manually," she said.

"Recounts serious matter," Rick Thurmond, The Sun Chronicle, November 18, 2000.
http://www.thesunchronicle.com/archives/ (Do search for: Rebecca Mercuri)

> Like it or not, mistakes are part of the system. Mistakes usually don't matter, the reasoning goes, because they are random and are spread across the ballot.
>
> "This goes on all over the country," said Rebecca Mercuri, a visiting professor of computer science at Bryn Mawr College in Pennsylvania and a frequent expert witness on computer security and voting systems.
>
> "Voting anomalies happen all over the country, in most states," she said. "Most voting systems have an error rate of between 2 and 5 percent. Most election officials will admit to that."

"Result? No one will ever know," Scott Shane, Baltimore Sun, November 14, 2000. Complete article is "Human and machine imperfections in the vote-counting process make a small degree of uncertainty inevitable." http://www.sunspot.net/content/archive/story?section=archive&pagename=story&storyid=1150510211886

> One person who has long tried to call public attention to voting system inconsistencies is Rebecca Mercuri, a computer scientist at Bryn Mawr College who has studied voting machines for a decade and defended her doctoral dissertation on "Electronic Vote Tabulation" at the University of Pennsylvania two weeks ago.
>
> "I couldn't get anyone to listen to me," she said yesterday. "Now my phone is ringing off the hook."

"Experts: Machine Counts Inaccurate," Tony Winton, Associated Press, November 11, 2000.

http://www.salon.com/politics/wire/2000/11/11/experts/index.html

> Problems with automated vote-counting equipment, especially the computer card punch type used in south Florida, have been well documented, said Rebecca Mercuri, a visiting professor of computer science at Bryn Mawr College.

Earlier Concerns

Although some articles in this section were written after the November 2000 election, the focus is primarily on earlier electronic voting issues.

"Internet Voting Project Cost Pentagon $73,809 Per Vote," John Dunbar, The Public i, August 9, 2001. The report to which this article refers can be found at: http://www.fvap.ncr.gov/voireport.pdf

> Rebecca Mercuri, an electronic vote tabulation specialist who founded the Notable Software consulting firm in Philadelphia, is an ardent critic of Internet voting. "The Internet itself is not secure," she said. "So there is no way you can make the product secure." Even encrypted messages are not safe when a computer is vulnerable to contamination, another expert noted.
>
> One of the biggest knocks against voting by computer is that it potentially excludes minority and low-income voters. "I'd rather see more money spent on sociological problems as opposed to spending $6.2 million" on Internet pilot programs, Mercuri said.

"Holes in punch-card system noted long ago," Jim Drinkard, USA Today, March 7, 2001. http://www.usatoday.com/news/politics/votingindex.htm/2100-03-07-voting.htm

> "It has always puzzled me why my report never got a wider acceptance," says Saltman, now 68 and retired. His 1988 report is gaining wide circulation, and he has been called as an expert witness before task forces and forums on what ails American elections. "It takes a crisis to move people, and it shouldn't have," he says.
>
> At a recent debate on computer voting technology in Washington, Bryn Mawr College computer scientist Rebecca Mercuri held up a copy of Saltman's 1988 report. "Those of us familiar with this document knew about these flaws all along," she said.
>
> When Saltman set out to study voting systems, little information was available, so he tracked down reports of local election foul-ups, interviewing the officials involved to identify what went wrong. That sounds elementary, but there was no central national agency to oversee elections -- a situation that hasn't changed.

"Computerized Voting Would be Fraught with Security Problems, Experts Say," Margie Wylie, Newhouse News Service, November 10, 2000.

> Closed systems -- in which voters don't cast ballots from their own PCs, but venture to the polls to make a purely digital vote -- aren't much better, said Rebecca Mercuri, a professor at Bryn Mawr College and forensic computer scientist who is finishing a doctoral dissertation about computerized voting.

> The systems themselves would be made up of millions of lines of code that could contain errors or be tampered with by any number of people involved in the voting process, from the manufacturer on down to local election officials, Mercuri said.
>
> She pointed to another Florida event -- the March 23, 1993 city elections in St. Petersburg -- as an example. In that case, during a test of two computerized vote tabulation systems, an industrial precinct in which there were zero registered voters showed 1,429 votes for the incumbent mayor. He won the election by 1,425 votes.
>
> Election officials later testified in court that the votes were consolidated from the two systems being tested, but they could never pinpoint the precincts from which the votes originated, Mercuri said.
>
> A recount ultimately confirmed the election's outcome. But there was no way to know what factor -- error or fraud -- caused the tabulation problem. ``The bottom line with computers is that there's no smoking gun, it just goes away,'' Mercuri said.

"New voting options, past and future. Use technology to change elections? Hardly a new idea," Lisa Napoli, MSNBC Opinion, November 8, 2000. http://www.msnbc.com/news/487467.asp

> The state of siege caused by this undecided election is all the proof we need that America must find a new way of casting ballots. And that new way should somehow involve the Internet. Of course, there are plenty of reasons why voting online isn't yet ready for primetime. It could provide a field day for teen-age hackers and terrorists, for one thing, and the Internet isn't yet in every home.
>
> "For an industrial precinct in which there were no registered voters, the vote summary showed 1,429 votes for the incumbent mayor (who incidentally won the election by 1,425 votes)," writes Rebecca Mercuri, then a research fellow at the University of Pennsylvania. "Officials explained under oath that the precinct was used to merge regions counted by the two computer systems, but were unable to identify precisely how the 1,429 vote total was produced. Investigation by the Pinellas Circuit Court revealed sufficient procedural anomalies to authorize a costly manual recount, which certified the results."

"Machine Politics," Michael Tomasky, The Village Voice, June 20, 1995.

> A number of people besides Kellner have raised concerns, mostly about ballot security. Rebecca Mercuri is a research fellow at the University of Pennsylvania who has worked in computer security for a variety of industries. She took an interest in computerized voting machines in 1989, she says, and has spent six years "reading, writing, and testifying" on the subject in many cities.
>
> "Sequoia Pacific hasn't satisfied its agreement" with New York City, Mercuri says. She says that SP and Deloitte & Touche, the accounting firm that is doing much of the systems programming, were supposed to deliver a "security and control document" that would describe how security would be delivered, what would happen in case of a breach, and so on. "It says none of those things," Mercuri says.

US Elections 2002

Sorry, this section is under construction. It will eventually provide coverage of 2002 election activity in the USA.

World Democracies

My October 2002 visit to the UK was, as the Cabinet Office said on their e-Democracy website "well publicised." Numerous media interviews generated the pieces below. The UK press is quite different from what I'm used to over here in the States -- some will track you down at your hotel at breakfast, schedule interviews and not show, and then quote or even rubbish you without ever having heard your position! Fun stuff. But for the most part, I was impressed by their enthusiasm and willingness to give fair treatment to a complex and controversial issue.

"E-voting increases risk of electoral errors and fraud, US expert warns," Bill Goodwin, Computer Weekly, 24 October, 2002. http://www.cw360.com/article&rd=&i=&ard=116852&fv=1

> The political interest in e-voting has been heavily influenced by the promises of IT and equipment suppliers that it will deliver more accurate and quicker election results at comparable or lower cost.
>
> This persuaded the Government to invest £3.5m in trailing electronic voting systems in the local elections in May this year. This month it issued an invitation to tender for further e-voting trials to begin in 2003. Public consultation is also under way.
>
> With the exception of the Electoral Reform Commission, which has raised questions about the maturity of e-voting technology, there has been barely a note of public dissent. But this week a world expert on e-voting, Rebecca Mercuri of Bryn Mawr College, Pennsylvania, urged Cabinet Office officials to think again.
>
> "It is a known fact that the computer industry does not have the capability, at present, to assure a safe reliable election using only electronic devices," she said. "Investigation of supplier claims and failures of performance in actual elections have demonstrated major flaws."
>
> Mercuri's contention is that e-voting systems present serious security risks and are much more vulnerable to fraud, manipulation and error than the paper-based equivalent.
>
> The laws of computing, she says, cannot allow anyone to be certain that the complex software needed to support e-voting is either fully secure or error free.

"E-voting developers dismiss criticism," Dinah Greek, vnunet.com, 21 October, 2002. http://vnunet.com/News/1136146

> Organisations working on electronic voting technology have dismissed criticisms that it is unsafe and fundamentally flawed.
>
> Fears were raised after Rebecca Mercuri, an assistant professor at Bryn Mawr College in Pennsylvania, told Cabinet Office officials earlier this month that e-voting systems are

dangerous.

She claimed that the systems fail to provide the necessary accountability, offer poorer reliability and provide greater opportunity for fraud than traditional methods.

Mercuri, who has also addressed the American Congress about potential security problems, said last week that people could not rely on the security of e-voting.

She also pointed out at two seminars organised this month in the UK by independent think tank, the Foundation for Information Policy Research, that websites set up for internet voting could be "spoofed" and were vulnerable to sabotage. However, Julia Glidden, managing director of Election.com, a voting software and services company, vehemently denied the accusations.

"Computer scientist rubbishes e-voting," Nick Farrell, vnunet.com, 18 October, 2002.
http://vnunet.com/News/1136112

A top computer scientist has warned the UK government that its plans for internet voting are a licence to commit election fraud.

Rebecca Mercuri, assistant professor of computer science at Bryn Mawr College in Pennsylvania, told The Guardian that she was horrified that any government would even consider using the internet for elections.

She explained that e-voting leaves no paper trail and provides less accountability, poorer reliability and greater opportunity for fraud than traditional methods.

Although people assume that electronic voting employs the same technologies used in everyday life, such as in banking or airline ticketing, Mercuri insisted that there are crucial differences.

She argued that internet voting is inherently unsafe because websites can be "spoofed, identities can be stolen and the whole thing is open to international attack".

Without using biometric techniques like iris or fingerprint scanning, Mercuri said that there is no way of establishing online that the person voting is who they say there are.

"Fears raised over e-voting," BBC News, 17 October, 2002, 10:36GMT.
http://news.bbc.co.uk/2/hi/uk_politics/2336023.stm

One of the world's leading experts on electronic voting is warning the government that computer polls cannot be trusted.

Rebecca Mercuri, assistant professor of computer science at Bryn Mawr College in Pennsylvania, is meeting officials at the Cabinet Office on Thursday. Voting through the internet or touch screens gives more chance for electoral fraud, says Ms Mercuri.

The warning comes as the government continues to consult the public and experts about

moves towards so-called e-democracy.

Ms Mercuri has already given evidence to the American Congress and now is bringing her research to the UK. She is giving a lecture, organised by internet think tank the Foundation for Information Policy Research, at the Royal Academy of Engineering on Thursday.

"Don't trust computers with e-votes, warns expert," Stuart Millar, The Guardian, October 17, 2002. http://www.guardian.co.uk/internetnews/story/0,7369,813223,00.html

A world experts in electronic voting will today warn the government that trusting computers with the democratic process is a recipe for fraud and error.

Rebecca Mercuri is assistant professor of computer science at Bryn Mawr College in Pennsylvania, who has given evidence to the US Congress. She is meeting the Cabinet Office in London today, and will urge reconsideration of alternatives to crosses on ballot papers, such as internet and text-message voting, because their results cannot be guaranteed to be secure and accurate.

She told the Guardian yesterday: "E-voting systems actually provide less accountability, poorer reliability and greater opportunity for fraud than traditional methods.

"People assume that electronic voting is just the same as other technologies we use in everyday life, like banking or airline ticketing, but there are crucial differences.

"With all these other systems there is a physical data trail, bits of paper that allow us to check that the transactions are accurate. E-voting offers none of these safeguards."

Ms Mercuri warns that no e-voting system exists that meets these tests.

Mercuri Biographical

These articles discuss Rebecca Mercuri's lengthy involvement in voting technology advocacy.

"'Scalable' Ballot Fraud: Why One Tech Maven Fears Computer Voting," Thomas E. Weber, Wall Street Journal, March 19, 2001. http://www.wsj.com

The transcript to the chat session hosted by WSJ On-Line (and referred to at the end of the article) makes for very interesting reading. Access it at: http://interactive.wsj.com/public/current/articles/SB985032601926471110.htm

PRINCETON, N.J. -- Rebecca Mercuri loves computers. But when it comes to counting votes in an election, she favors plain old paper. Computers, she says, just can't be trusted with our democracy.

"I fear for what's happening," says Ms. Mercuri, a 46-year-old authority on voting systems whose expertise is suddenly in great demand. Ms. Mercuri is no Luddite. She has programmed for decades and teaches computer science at Bryn Mawr College. Nonetheless, she says, "the idea of running an election on the Internet is totally

> horrifying."

"Rebecca Mercuri: BMC's Electronic Voting Expert," Juliana Rosati, Bryn Mawr College News, March 7, 2001 Volume XXIII, No. 9 (cover story). http://bartik.brynmawr.edu/orgs/cnews/3.7.01/mercuri.html

> It was the Sunday after the as-yet-undecided 2000 presidential election. As the nation wondered in tense disbelief when it would finally know the name of its next president, the telephone rang at Bryn Mawr Computer Science professor Rebecca Mercuri's home.
>
> "I pick it up, and this guy identifies himself as an attorney for the Vice President," she recalls. Laughing, Mercuri remembers her initial moment of unspoken amazement.

"Technology & the Polls: Rebecca Mercuri," Douglas Dixon, U.S. 1 Newspaper, November 15, 2000 (cover story). http://www.princetoninfo.com/200011/01115c01.html

> The paper process can be slow and inaccurate, but the digital replacements also have problems. "People see Internet voting as a solution," says Rebecca Mercuri, an expert on voting security. "It's chilling. It will compromise voter anonymity and auditability. It would solve the recount problem, because we won't be able to do a recount."

Sound Bites and Video Clips:

The PC Radio Show, WBAI 99.5 FM (New York, NY), Wednesdays 8-9PM ET. Rebecca Mercuri is their special correspondent with a monthly feature on voting technology. Broadcasts can be listened to via the "Recently Mentioned on the Show" link or "Show Archives" at http://www.pcradioshow.org. (February 11, 2004: The Internet Voting SERVE Project.)

Morning Edition with David Kestenbaum, NPR, "Experts Warn of Electronic Voting Security Risks," December 12, 2003. Radio interview including quotes with Rebecca Mercuri is archived at http://www.npr.org/features/feature.php?wfId=1545294. *U.S. election officials and computer scientists met in Maryland this week to discuss the merits and pitfalls of electronic voting. Proponents say computerized voting systems will simplify the tallying of votes. But many computer experts fear the technology will allow vote tampering.*

This American Life, WBEZ/NPR (Chicago, IL), Episode 250, "The Annoying Gap Between Theory ... and Practice," November 7, 2003. Act One features Rebecca Mercuri (16 minutes of audio), available from http://www.thislife.org. *Why is it always harder than you think it'll be? We explore several case examples: Act One. Rock, Paper, Computer. Reporter Jack Hitt explains the alarming difference between theory and practice when it comes to computerized voting machines. Specifically, those made by a company called Diebold.*

The Center for Investigative Reporting and American RadioWorks, "Whose Vote Counts?" a featured story, part of Minnesota Public Radio's special coverage "Whose Democracy is It?" broadcast during November 2003. "The Promise of Electronic Voting" radio documentary featuring Rebecca Mercuri, can be ordered from http://www.americanradioworks.org/features/voting/, and the transcript can be

read at http://www.americanradioworks.org/features/voting/transcript.html. *Counties across America are getting rid of their old punch card ballots and installing high-tech voting machines. But some computer scientists worry that the new systems could be vulnerable to fraud.*

"Voting Machines: A Threat to Democracy?" forum in Philadelphia, PA, September 7, 2003. A video is available, featuring Rebecca Mercuri, Marc Rotenberg, Ina Howard and Lynn Landes, ordering information at http://ecotalk.org/ForumPressRelease.htm. *Voting machines and the private companies that sell and service them control the casting and counting of votes in over 98% of all elections in the United States, and in many countries around the world. Concerns about the security and integrity of elections are mounting among computer experts, politicians, and citizens. Most forums on this subject have concentrated on technical issues only. This distinguished panel of experts will address the technical, constitutional, and political aspects of voting by machine.*

New Focus with Mike DeRosa, WWUH 91.3FM (West Hartford, CT), May 16, 2003. Part Two of a 3-part radio series on Black Box Voting, featuring Rebecca Mercuri, is archived at http://www.newfocusradio.org/audio_archive.html.

Morning Edition with Dan Charles, NPR, "Electronic Voting Machines Unreliable, Some Experts Say," February 10, 2003. Radio interview featuring Rebecca Mercuri and Peter Neumann archived at http://discover.npr.org/features/feature.jhtml?wfId=990452. *State and local officials buy electronic voting machines in hopes of avoiding the low-tech messiness of pencil marks on paper ballots and so-called "hanging chads." But some computer scientists say vote-counting computers are inaccurate.*

WAMU Radio (PBS) from American University, "Public Interest", November 14, 2000. This hour-long radio broadcast hosted by Kojo Nnamdi, featuring Rebecca Mercuri, Kim Alexander, Jim Adler and Curtis Gans, is archived and can be heard at http://www.wamu.org/pi/shows/piarc_001113.html#tuesday. *Last Tuesday, more than half of America used voting technology developed in the 19th century -- mechanical hand levers and punch cards. As the controversy over ballot confusion and recount delays continues, we'll look at the future of voting in the age of the digital revolution.*

<-- Return to Electronic Voting Homepage