The Atlantic

The Computer Scientist Who Prefers Paper

Barbara Simons believes there is only one safe voting technology.

John Cuneo

JILL LEOVY | DECEMBER 2017 ISSUE | TECHNOLOGY

FOR YEARS, Barbara Simons was the loneliest of Cassandras—a technologist who feared what technology had wrought. Her cause was voting: Specifically, she believed that the electronic systems that had gained favor in the United States after the 2000 presidential election were shoddy, and eminently hackable. She spent years publishing opinion pieces in obscure journals with titles like *Municipal World* and sending hectoring letters to state officials, always written with the same clipped intensity.

Simons, who is now 76, had been a pioneer in computer science at IBM Research at a time when few women not in the secretarial pool walked its halls. In her retirement, however, she was coming off as a crank. Fellow computer scientists might have heard her out, but to the public officials she needed to win over, the idea that software could be manipulated to rig elections remained a fringe preoccupation. Simons was not dissuaded. “They didn’t know what they were talking about and I did,” she told me.

She wrote more articles, wrote a book, badgered policy makers, made “a pain of myself.” Though a liberal who had first examined voting systems under the Clinton administration, she did battle with the League of Women Voters (of which she is a member), the ACLU, and other progressive organizations that had endorsed paperless voting, largely on the grounds that electronic systems offered greater access to voters with disabilities.

Simons was called a Luddite. At times, she was treated as just short of raving. At a League of Women Voters convention, she took a turn at the microphone to challenge the league’s president. The moderator tried to yank the mic from her hand.

Simons is not grappling for mics anymore. In late July, at the annual Def Con hacker conference, in Las Vegas, she addressed an event called the Voting Village—a staged attack on voting machines. "I lose sleep over this. I hope you will too," she told the hackers who had packed into a windowless conference room at Caesars Palace.

Four voting machines had been secured for the event, three of them types still in use. One team of hackers used radio signals to eavesdrop on a machine as it recorded votes. Another found a master password online. Within hours of getting their hands on the machines, the hackers had discovered vulnerabilities in all four.

For much of the afternoon, Simons was in the pressroom, surrounded by reporters eager to hear her make the same points she'd been making for years. "Anything that's happening in here, you can be sure that those intent on undermining the integrity of our election systems have already done," she told a reporter from *USA Today*.

Russia's efforts to influence the 2016 presidential election have reversed Simons's fortunes. According to the Department of Homeland Security, those efforts included attempts to meddle with the electoral process in 21 states. At the same time, a series of highly publicized hacks—at Sony, Equifax, the U.S. Office of Personnel Management—has driven home the reality that very few computerized systems are truly secure.

State officials now return Simons's calls. Like many of her former adversaries, the League of Women Voters no longer insists on paperless voting. In September, after years of effort by Simons and the nonprofit she helps run, Verified Voting, Virginia abandoned the practice. I asked Simons how it felt to be vindicated. "It sucks," she said. "I would much rather have been wrong."

Evidence has yet to emerge that Russia successfully manipulated voting systems in 2016, and most of Russia's probing appears to have been aimed at databases of registered voters, not the machines that record votes. But Simons believes that the failure to heed her warnings has left states in grave danger, with too many potential weak points to shore up before hackers do succeed in altering an outcome. It is not a theoretical vulnerability, Simons told me. "Our democracy is in peril. We are wide open to attack."

"It's not that I don't like computing or I don't like computers. I mean, I am a computer scientist," she said. "Many of the leading opponents of paperless voting machines were, and still are, computer scientists, because we understand the vulnerability of voting equipment in a way most election officials don't. The problem with cybersecurity is that you have to protect against everything, but your opponent only has to find one vulnerability."

Simons is slight of build, with short auburn hair. She walks and speaks at a breakneck speed that suggests her urgency of purpose. On a recent weekday, she touched down at Los Angeles International Airport wearing knee-high suede boots. She was in town for a meeting with the television star turned activist Alyssa Milano, one of many high-profile figures now eager to tap Simons's expertise.

Milano wore her own boots, in metallic gold. Sitting at a conference table in the monumental headquarters of Creative Artists Agency, Simons addressed the actor and her entourage in typically blunt fashion. "I'm scared shitless," she said.

Simons told Milano what she's been telling state officials from Rhode Island to California: We have a single technology at our disposal that is invulnerable to hacking—paper. Verified Voting's goal is to get paper ballots in every state.

Where the organization meets resistance, it funds local activist groups and hires lobbyists; where it finds a sympathetic ear, it provides technical expertise and a road map for creating a secure system.

By Verified Voting's count, 13 states, including populous ones such as Pennsylvania and New Jersey, still have paperless voting. Given the thin majorities in Congress, that leaves more than enough machines to allow hackers tremendous power to influence American politics. And all 50 states use computerized scanners for vote counting—few of them with sufficient postelection auditing to detect manipulation. Mandatory audits, in the form of hand counts of randomized samplings of ballots, are essential to protect against invisible vote theft, Simons believes. In an unaudited system, malicious code could easily go unnoticed. "It's not rocket science," she said. "Any halfway-decent programmer could do it."

BARBARA SIMONS IS one of the original figures in a movement of perhaps three dozen people who have been fighting for paper ballots for nearly two decades. None are yet accustomed to being taken seriously. When Verified Voting first started working in Virginia, it was seen as "kind of out there," admits Edgardo Cortés, the commissioner of Virginia's Department of Elections. Now "they're on the top of the list of who we call."

Leading up to September's unanimous, bipartisan decision by the Virginia board of elections to decertify the state's remaining touch-screen voting machines, Simons was in the thick of the debate, emailing back and forth with election officials as they sought to assess the vulnerability of paperless machines. Cortés remembers that Simons "butted heads with a number of election officials over the years." But, he adds, "I think her passion to keep pushing the issue over time—to just continue—it's had results. It really changed things."

What needs changing is a system that took root after 2000, when the presidential election hinged on the infamous chads left behind by Florida voters. Computer voting was still novel at the time, but it seemed like an improvement on the antiquated punch-card systems used in places like Broward County. If not properly maintained, those machines produced less-than-clean punches and ambiguous (“hanging,” “pregnant”) chads. “The takeaway was that paper ballots weren’t any good,” Simons recalled.

In 2002, Congress passed the Help America Vote Act, and suddenly states were awash in money to invest in new systems—and fearful of becoming the next Florida. Security was a secondary concern—even though many of the new machines had wireless features and left no paper trail. They were viewed as easier to use, and seemed to have little downside. Each state “wanted to get the newest and greatest shiny object,” said Simons. It was “a gold-rush mentality.” She still has a League of Women Voters statement supporting the paperless revolution in which “hacking”—rendered in scare quotes—is quickly dismissed as a concern.

At the peak of the electronic-voting revolution, in 2006, some 40 percent of registered voters used paperless machines. Verified Voting worked to stem the tide, but found little receptiveness for its dark visions of compromised machines. Kevin Shelley, California’s secretary of state from 2003 to 2005 and a supporter of paperless voting, reluctantly took a meeting with Verified Voting. The group he’d dismissed as “crazy activists” made a compelling case, backing it up with data and reports on the insecurity of paperless machines.

“There’s no malware that can attack

paper.”

Shelley changed his position, and California became an early, important victory for the group. Thanks in part to California’s shift, enthusiasm for electronic systems abated elsewhere, but not before thousands of machines were ensconced across the country.

Verified Voting supports some machine systems—hybrid models that ink paper ballots and can help people with disabilities to vote—so long as the results are audited. But Simons stubbornly prefers pen and paper, which she believes is the simplest, most idiotproof system. Of course, all voting systems must contend with the grubby realities of democracy—design and function have a way of diverging when millions of people enter the equation. Douglas Jones, a computer scientist who co-authored a book on voting history with Simons, notes that a surprising number of Americans insist on exercising their franchise using glitter pens.

What paper boasts—and no existing computer system can rival—is a solution to the confounding logic problem at the heart of our electoral system. The secret ballot presents a paradox: How can the validity of each vote be confirmed without being traceable to any individual voter? Ballots must be “anonymous and yet verifiable, secret and yet accountable,” says Eric Hodge of CyberScout, a security-services company that advises states and counties.

Paper, Simons said, is the best answer to this riddle. Marked clearly and correctly, it’s a portable and transparent record of voter intent, one that voters themselves can verify, at least while the ballot is still in their possession. It’s also a permanent record, unlike computer memory, which can always be overwritten.

“There’s no malware that can attack paper,” Simons said. “We can solve this. We know how to do it.”

The promise of practical results—of solvable problems—is one of the things that first lured Simons to computer science, in the early 1970s. She was one of just a few women in UC Berkeley’s doctoral program. She concentrated on a programming challenge called “scheduling”—the mathematical sequencing of tasks. She was certain that she could solve the problem she set before herself in writing her thesis, and she did, after two years of intensive research.

Repairing America’s voting system has been less hermetic work, and the results have been more mixed. A few weeks after her victory in Virginia, Simons fought, unsuccessfully, against a measure in California that rolled back audit requirements she’d wanted to strengthen. But Simons has come to see politics and persuasion as essential to her discipline. “The technical community has a responsibility to inform policy makers of the limitations as well as the benefits of technology,” she said. “That is part of engineering.”

ABOUT THE AUTHOR

JILL LEOVY is the author of *Ghettoside: A True Story of Murder in America*.