



Is Secure Online Voting Too Good To Be True? (For This Company, It Might Be)

by Chitra Ragavan · 03 Feb 2021 · 25 min read

When [Amelia Powers Gardner](#) won political office as [county clerk and auditor](#) in Utah County, Utah, in January 2019, she was determined to fix what she viewed as the county's archaic and dysfunctional voting mechanisms.

Around that same time, nearly 800 miles northwest, [Christine Walker](#), the long-time [county clerk](#) in Jackson County, Oregon, had been deploying various hardware and software products to revamp her county's voting technology and processes with little success. She was ready for something new.

Walker and Gardner don't know each other. But when they each learned about a small Boston-based tech startup, called [Voatz](#), that had built the first mobile voting app and platform secured by blockchain technology, they were immediately intrigued. And upon

discovering that West Virginia and Colorado were already testing the app for absentee military voters overseas, the two election leaders were even more eager to put their counties on the map as trailblazers in online voting.

“I like to be the person that's kind of setting the pace, not just following along,” says Walker, who prides herself on her tech-savvy leadership. Gardner, a former Caterpillar executive, automotive technologist, and business efficiency expert, is similarly technologically inclined.

“It piqued my interest because not only is it blockchain and I’m a bit of a blockchain nerd,” Gardner says, “But also because it seems like a more secure, more simple way, more reliable way for these underserved and disenfranchised citizens to cast their votes.”

The Reality, However, May Be Anything But Secure

Noble intentions aside, Walker and Gardner’s vote of confidence in Voatz may be misplaced, say members of the cybersecurity community who have repeatedly warned the U.S. government that the app is vulnerable to hacking. These experts, along with several members of Congress, have criticized Voatz for its failures in transparency, lack of accountability, and refusal to release its source code so that it can be better tested for security flaws.

“I struggle to find anybody in the information security community that has anything good to say about them,” says [Tarah Wheeler](#), a Belfer fellow in cybersecurity at Harvard University, an international security fellow at New America, and a Fulbright scholar.

Voatz’s CEO and co-founder [Nimit Sawhney](#) asserts that his startup is deeply committed to security and that his mobile voting app is secured with the best “military-grade technology available, including biometric identification, cryptography, and blockchain.”

He says the voting platform “has successfully defended itself against 100% of the cyber attacks directed at it.” Sawhney believes that, “a lot of claims have been theoretical: X, Y, Z could happen. And, in theory, a lot of bad things can happen with in-person voting and with postal voting as well. But we still, you know, use them.”

But information security experts describe the conundrum with Internet voting as so “fundamental” and “inherent” that even the best cryptographers and systems security researchers have failed to solve it, literally for decades, despite intense and focused efforts. “Any product claiming to have solved this problem is therefore making an extraordinary claim,” says [Michael Specter](#) of the Massachusetts Institute of Technology (MIT), who has extensively analyzed Voatz and other Internet voting technologies. “Attacks on Internet voting systems are scalable (allowing one attack to change many ballots rapidly and undetectably), remote (can be conducted from pretty much anywhere with an internet connection), and relatively cheap,” Specter says, whereas, “Attacks on in-person voting, if done properly with the right set of tools, is auditable and really expensive to attack, often requiring physical access and many human failures to change an election outcome.”

Indeed, despite the scores of last-ditch, politically motivated, in-person voter fraud allegations leveled by former President Donald Trump and his attorneys in last year’s Presidential race, won by Joseph R. Biden, the Washington Post [reported](#) that “in a remarkable show of near-unanimity across the nation’s judiciary,” 86 judges ranging from state courts to the Supreme court strongly rejected every single fraud allegation. And the [Department of Homeland Security](#) declared the November 3rd elections as “the most secure in U.S. history.”

Between A Rock and A Hard Place

The security concerns and controversies swirling around Voatz highlight the extraordinary challenges confronting the U.S. government as it attempts to modernize

the nation's archaic voting mechanisms at a time when voting rights are proving to be an increasingly explosive issue. That's evidenced by the violent and bloody January 6 riots on the U.S. Capitol, instigated by Trump, culminating in his second, historic impeachment by the House of Representatives, with conviction proceedings to commence next week in the Senate. The Voatz saga exposes the deep rifts between tech startups, governments, and information security communities regarding the safety and efficacy of online voting—specifically mobile voting technologies. And it demonstrates the challenges confronting local elected officials such as Walker and Gardner, who find themselves between a rock and a hard place in evaluating and picking from the very limited choices of Internet voting technologies and parsing the often-opaque marketing claims of ambitious startups such as Voatz. These officials must balance the conflicting tensions between complying with [federal law](#)—which requires that electronic ballots must be sent to all military and disabled voters overseas—and laws in 32 states, including Utah, that also require the electronic return of ballots, all the while expanding access to underserved voters while at the same time ensuring ballot security and integrity.

The alarming cyber vulnerabilities of American elections were first exposed by the [2016 Russian hacking](#) in the U.S. presidential elections and led the National Academy of Sciences to issue a strongly worded [report](#) in 2018 that warned against sending electronic ballots by Internet. “No current technology,” the report read, “can guarantee their secrecy, security, and verifiability.”

The continued boldfaced Russian, Chinese, and Iranian [interference](#) in last year's presidential elections, in addition to the recent months-long [SolarWinds hacking](#)—reportedly Russian-led and penetrating multiple U.S. government agencies—only served to further exacerbate those concerns. Sawhney blames the decades-long institutional resistance against Internet voting for the blowback against Voatz.

“Many researchers have taken an absolutist position declaring that Internet voting is not secure,” says Sawhney.

“This blanket statement does not consider the recent developments in technology or advancements in security. The cost of holding back innovation in voting is continuing to disenfranchise voters.” - Nimit Sawhney

While Voatz is an early entrant in the space and the only blockchain mobile voting app, it is confronting stiff competition from [equally challenged](#) electronic voting alternatives, notably the web-based OmniBallot platform from [Democracy Live](#) and [TXT2VOTE](#) from mobile marketing giant, [Global Mobile](#).

The Story of Voatz

For Sawhney and his brother Simer, who is a Voatz co-founder, the idea of using blockchain technology to secure votes arose from dark memories of elections in India, where they grew up in the minority Sikh religion during a violent and pivotal point in the nation’s history.

Three decades later, in 2014, when Sawhney and Simer were both living in the U.S. and working in tech, they attended the “Hack to the Future” software hackathon at the [South by Southwest](#) tech and culture fest. Struck by the data security aspects of blockchain technology—especially the ability to create an immutable and permanent record of transactions—Sawhney and his brother prototyped a smartphone-based voting system that used biometrics, ID verification, and a system to record ballots on the blockchain. He now recalls this as the “accidental origin” of Voatz.

“When we presented it on stage, it was pin-drop silence, like we had completely

bombed it,” says Sawhney. He was shocked when they were announced as the first prize winners—in part because the idea itself “seemed so audacious to us at the time.” So audacious that he says even one of the judges, a venture fund investor whose name he declined to provide, told them it would be futile to further pursue the idea.

To clarify, a blockchain is a “digital ledger” that most people associate with cryptocurrency like bitcoin and other digital assets, but it can also be used to record any kind of electronic transactions, including the casting of ballots, in a permanent, secure, transparent, and tamper-proof way. In theory, that makes it very attractive for electronic voting, where security is paramount. But, in reality, blockchain is still very much aspirational technology with few proven results in the governmental space today, says civic technologist and open government hacker, [Joshua Tauberer](#).

“Today, blockchain has been around for a decade, maybe more than a decade,” says Tauberer. “I have never seen any product or project that solved a civic problem that’s used blockchain.”

Despite all this, the Sawhney brothers decided to buck the odds. They moved forward with building the Voatz platform and app, realizing that they could vastly increase access to voting for both citizens abroad and people with disabilities.

To date, Voatz has conducted a total of 76 big and small elections with 270,174 votes cast — including in churches, unions, universities, and towns, both major political party state conventions and governmental elections — and even a national referendum in Venezuela. Of those 76 elections, 14 were U.S. governmental elections with 1994 voters. Of those 1994 voters, 1151 voters used Voatz in Utah and Oregon in the first blockchain-backed smartphone app voting exercise in the Presidential elections last November. To date, Voatz has won numerous civic tech innovation awards and says it has raised \$9.2 million in capital as it seeks to expand its footprint.

Mounting Concerns

The biggest threat confronting Voatz is the startup's aggressive posture towards and corrosive relationship with the information security experts, academics, researchers, and ethical hackers that have raised questions about its security risks and practices.

In May 2019, five academic, election, and research organizations led by Lawrence Livermore National Laboratory released a 10-page list of questions called, "[What We Don't Know About the Voatz "Blockchain" Internet Voting System.](#)" The report criticized Voatz for its lack of transparency surrounding its technology: "While much of this secrecy might be understandable for an ordinary business product and service, it should not be acceptable in a public voting system whose details should be transparent to voters, candidates, and the public at large." Six months later, [Sen. Ron Wyden](#) (D-Oregon) wrote a [letter](#) to the heads of the Department of Defense and the National Security Agency taking aim at the company's "level of secrecy" about its security auditors and their findings and urging these agencies to conduct a cybersecurity audit to determine if Voatz was vulnerable to foreign hacking.

In December 2019, a month after Sen. Wyden's letter, Voatz and the non-profit [Tusk Philanthropies](#), a funder of online voting projects, hired [Trail of Bits](#) to conduct what the cybersecurity firm described as "the most complete security assessment of the platform to date." Trail of Bits said Voatz gave "unprecedented access" to nearly 200,000 lines of "pure source code" to conduct the first "white box assessment, scoped to include the discovery of Voatz Core Server and backend software vulnerabilities."

Even as the Trail of Bits security analysis was underway, on February 6, 2020, Sen. Wyden sent another [letter of concern](#), this time to Oregon's Secretary of State urging him to reconsider his decision to use Voatz without seeking "advice or an evaluation" from the federal government or independent security experts.

Meanwhile, Voatz became [embroiled](#) in a controversy with the ethical hacker community that further underscores the company's issues with transparency. It's customary for tech companies to offer rewards and protection from prosecution to ethical hackers for hacking into their software through specialized platforms like HackerOne to help them find bugs. However, Voatz reported two University of Michigan students who were trying to do a security analysis of the app, believing they were operating under those terms.

In a [legal brief](#) filed in an unrelated lawsuit, Voatz explained that the incident was reported to its customer, the State of West Virginia, who in turn reported it to the FBI, because the "students' ill-advised activity was indistinguishable from a hostile attack," and that "students did not seek any prior authorization privately or through Voatz's bug bounty program." But Wheeler who has tracked and documented the controversy and other information security experts say Voatz [retroactively narrowed](#) the safe harbor terms of its bug bounty program, exposing the Michigan students to potential criminal prosecution.

For Voatz, this was one of many self-inflicted wounds that have led to a rupturing of trust and credibility and rendered the startup radioactive in the information security communities whose goodwill it will need for long-term success in the election-tech space.

The Truth Is in the Tech

As these concerns were coming to a head, Specter—a member of the Internet Policy Research Initiative and the Computer Science and Artificial Intelligence Laboratory at

MIT, and a research affiliate at Google—had already spent a year examining whether blockchain technology, in general, had any value in elections. His team ultimately found blockchain to be ill-suited for the task, which is why he became curious about Voatz's

blockchain claims and decided to veer off the broader blockchain project and focus specifically on Voatz.

The two questions that the MIT researcher wanted to answer was how the company was using blockchain technology, if any, and how adversaries with various types of powers could potentially manipulate the app to subvert the legitimate outcome of elections. Not having access to the source code and concerned about potential legal ramifications—partly stemming from Voatz’s problematic legal history within the ethical hacking community—Specter began reverse-engineering the app. “And then I started getting more and more afraid of what I was seeing,” Specter recalls. “As time went on, it just became very clear that the product was not secure and was doing the things that are antithetical to privacy as well.”

“What we found with Voatz in particular was that an adversary that controlled your phone could do anything to you they wanted,” Specter says. “But worse than that, we found that a passive network adversary, so someone who is just watching you on your network, say at an insecure coffee shop wifi that you’re using to vote or on the insecure router that you’re using to connect to the Internet at home, could be spying on the way that you voted.”

Even more concerning, says Specter, was his finding that the app was also vulnerable to insider threats. An adversary with access “could vote for you in any way it wanted to,” he concluded. Even worse, there was no way for voters to know that their ballot had been changed. “So in essence, Voatz itself, the company, could actually control the entire election if they were used for every voter,” Specter continues, “and that is kind of a worrying power to give one company in a digital sense.”

Specter also found that the Voatz app could pose dangerous privacy issues for voters, particularly U.S. military personnel deployed in hostile zones. The company had previously failed to disclose that it was allowing a third-party vendor to access personal data for voter identification and verification purposes including Voter IDs, selfie photos,

and worse yet, GPS locations. “Given what I have seen, I would not recommend Voatz to anyone and I certainly would not recommend the use of any Internet voting scheme that is not open source, that is not available for examination,” Specter concludes, “And I would not adopt anything that’s had the sort of problems this particular app has had without being able to verify that it’s actually been solved.”

A month after Specter’s MIT report was [released](#) last February—which Voatz staunchly [rebutted](#), not disputing the findings so much as criticizing the “erroneous method,” that it blamed for “false assumptions”—Trail of Bits, the security firm that Voatz itself had hired, released its own findings. The two-volume report, commissioned by Voatz in December 2019, included 116 pages of [technical findings](#) and 73 pages of [threat model](#) findings.

In a [blog post](#) confirming all of Specter’s findings at MIT and more, Trail of Bits explained the significance of its analysis, noting that five prior “black box” security audits “could not quell a great deal of uncertainty and public speculation about Voatz’s implementation and security assurances.” Trail of Bits said it had conclusively found 79 vulnerabilities, two-thirds of which were of “high” and “medium” severity and the remainder “a combination of low, undetermined, and informational severity.”

“Our assessment confirmed the issues flagged in previous reports by MIT and others, discovered more, and made recommendations to fix issues and prevent bugs from compromising voting security,” the blog post stated. “That includes the assertion that hackers could potentially change or discard votes.”

Trail of Bits described Voatz’s code as “unusually complex, with an order-of-magnitude more custom code than similar mobile voting systems we have assessed.” The blog post stated that Voatz’s code was “written intelligibly, and with a clear understanding of software engineering principles,” and that it was “free of almost all the common security foibles.” But the blog post noted that Voatz’s codebase was the “product of fast-paced

development. It lacks test coverage and documentation.” That failing is not uncommon in tech startups that pride themselves on the “move fast, break things,” ethos but in the election context, has alarming ramifications.

Trail of Bits concluded that the “quantity of findings discovered during this assessment, the complexity of the system, and the lack of access to both a running test environment as well as certain codebases leads us to believe that other vulnerabilities are latent.”

Last March, in a [blog post](#) responding to the Trail of Bits audit, Voatz described its collaboration with the security company as a “shift in the paradigm” and “an important milestone” in its efforts to “chart a new, forward approach to transparency in our elections infrastructure,” transparency that Voatz said, “is not always championed across the industry.”

Voatz also subsequently released a detailed mitigation [report](#) stating that of the 79 findings, the startup had resolved 20 of the 48 issues that it deemed relevant.

The Trail of Bits confirmation of the MIT findings and more, was a “really bizarre course of events,” says Specter.

“To this day, the company still doesn’t acknowledge that the vulnerabilities we found are real,” Specter continues, “even though a third party company which they hired and paid for and gave full source code for, confirmed everything that we found.”

Voatz’s conflicts with researchers and ethical hackers also came to a head last March when, in an unprecedented move, [HackerOne](#) bounced Voatz off its bug bounty platform—a first in its eight-year history—citing the startup’s hostile “pattern of

interactions” as cause for the termination. Voatz said the platform had bowed to [pressure](#) from “a small group of researchers” who were miffed over the University of Michigan incident.

Can the Ends Justify the Means?

Surprisingly, despite the crescendo of criticism and the hundreds of pages of technical reports documenting deeply troubling security flaws, Voatz still found willing and hopeful government partners in Gardner and Walker, the county clerks in Utah county, Utah, and Jackson County, Oregon. And to this day, they continue to defend the Voatz pilots as the best of a handful of imperfect solutions available to them to comply with federal and state electronic ballot requirements for underserved voters. Until recently, says Gardner, Voatz was the only online voting technology that could be used both domestically and overseas that also had independent third-party audit capabilities.

In terms of political experience, the two women are decades apart. Walker is an old hand at politics, having been reelected county clerk three times since she took office in 2008. In contrast, Gardner came in as a newbie at full-time politics though she had volunteered her time before. “I literally had no clue what to expect when I ran for office,” she says candidly.

Other than the disparity in their years of government service, Gardner and Walker actually have a lot in common. Both are registered republicans with a stated commitment to carrying out their duties in a non-partisan manner, as mandated by law. Both were elected with wide margins. Both come from humble working-class backgrounds and have lived hardscrabble lives.

Walker entered government service more than two decades ago after she struggled to make ends meet for herself and her young son. “I needed stability for him, I needed

insurance,” Walker says. “I needed a job that I knew I could put food on the table and a roof over our head.” Besides, Walker’s family has a long history of public service from her great grandfather, who was elected Jackson County sheriff in 1912 and was killed in the line of duty a year later, to her uncle, a former county commissioner.

Gardner is the youngest of five kids raised by a single mother who has congenital blindness and became disabled after a visitor to their home accidentally shot her with her own loaded M-16 rifle when Gardner was in first grade, confining her mother to a wheelchair and crutches for most of her adult life. Despite her seemingly insurmountable challenges, Gardner’s mother put herself through college and worked ceaselessly to support her large family while grappling with poverty and homelessness. It wasn’t until Gardner was in junior high that her mom had the means, ironically through the insurance payment from the gunshot incident, to buy a reliable car and a house, ending their period of homelessness.

Both Walker and Gardner say their experiences with adversity have given them the desire and determination to bring those on the edges of the American electorate, especially military personnel posted abroad, into the fold.

“After all,” says Walker, “They’re fighting and they are serving their country for the very right we’re discussing today.”

A final commonality is that both women are confident in their technical savvy and willing—even eager—to test out bleeding-edge technologies like Voatz that could help them in their mission to make voting accessible to all Americans.

Gardner had seen the challenges confronting U.S. absentee voters during the 2008 presidential elections firsthand when, as an expat living in Canada, her absentee ballot for the general election never arrived by mail. After taking office, she soon learned that

her second in command, Josh Daniels, had not received his primary ballot by mail either in 2008 when he was a Marine serving in Fallujah, Iraq. So Gardner and her deputy decided that revamping the absentee ballot mechanisms for uniformed and overseas citizens, or so-called [UOCAVA](#) voters, was their [top priority](#). In 2019, Utah County became the third jurisdiction in the country, after West Virginia and the City and County of Denver in Colorado, to deploy mobile absentee voting for these Americans living abroad.

The Suffragettes' Gift, Not To Be Squandered

Gardner then decided that the next order of business was to put her county on the map as the first in the nation to use mobile voting for constituents with disabilities, voters like her mother. Soon enough, she was connected with Utah County's oldest resident, Maude "MacCene" Maynard Grimmatt, who had been homebound for two years with a broken ankle that refused to heal due to her advanced age.

MacCene Grimmatt was born in 1913, seven years before women even had the right to vote. She was determined not to squander the hard work and sacrifices the suffragettes had made for decades to win that precious right for all women. Since Grimmatt first became eligible to vote, she had cast her ballot in every single election for nearly a century. For her, it didn't matter what technology was used. Indeed, she had little interest in what a blockchain was; she just wanted to find a way to cast her ballot despite her broken ankle. In Grimmatt, Gardner had found the perfect poster child—or rather, poster great-grandma—for her ambitious goal.

On November 5, 2019, MacCene Grimmatt, Utah's oldest active voter, used the world's newest mobile voting technology to [cast her ballot](#), making national news. With a push of a button, she took part in Gardner's [bold experiment](#), voting from the comfort of her russet couch in the Provo home where she had lived for most of her life.

“It’s pretty cool, isn’t it?” she remarked with a broad smile to the [Fox News](#) reporter who was there recording the momentous occasion. The Voatz app enabled MacCene Grimmett to vote not just in the municipal election that November but also in the 2020 presidential primary last March and the nominating primary in June 2020. All that time, though unbeknownst to Grimmett, a storm of controversy was brewing in tech and cybersecurity communities surrounding the app.

Bunch of College Students

Voatz’s Utah champion, Gardner, says she read the MIT and Trail of Bits reports in detail and raised the security issues “point by point” with Voatz and also has had conversations with MIT’s Specter, though he describes them as cursory at best. He wishes that election officials such as Gardner would trust the expert advice of information security experts such as himself but that seems unlikely to happen.

Gardner dismissed Specter and his team in a recent county [committee meeting](#) as “a bunch of college students who really have no clue how we run elections.” She says election officials “routinely share” voter data via secure networks with third party vendors. Sending completed ballots via email attachments is the least secure method of voting, she says, and in-person voting would not help her fulfill her Constitutional duty to help millions of underserved voters like Grimmett. “As an election official, I’ll be damned if I let some person on the East Coast tell me that I should restrict MacCene’s right to vote,” she recalls thinking. “At that point, I mean, the spitfire came to me where I said, ‘I want to find every underserved population and I want to make sure that in today’s world that they have the ability to vote.’”

It should be noted that Gardner is a long time friend of [Jonathan Johnson](#), CEO of Utah based Overstock, and President of Medici Ventures, a major investor to the tune of \$2.2 million, in Voatz. Johnson, who publicly [defended](#) Voatz in response to a negative story in the [New York Times](#) in the wake of the MIT report last February, contributed \$1500 to

Gardner's [political campaign](#) in 2018. She says she did not learn about Voatz from Johnson, that their friendship and interest in blockchain technology long precedes Voatz and that she defers final election technology decisions to experts in her office.

Gardner is supporting legislation to expand Voatz statewide but also says she's currently working with Global Mobile to implement their TXT2Vote product as an alternative for U.S voters with disabilities, and she's in talks with Democracy Live to use their remote balloting as an option for overseas citizens. "We are constantly looking for and evaluating products so that we can provide the best options to our citizens," Gardner says.

MIT's Specter maintains that the only safe alternatives to in-person voting today is vote by mail, braille ballots, and Remote Accessible Vote By Mail (RAVBM) systems that deliver ballots digitally, but require the user to print out the ballot and mail it in.

Over in Jackson County, after seeing a trade show presentation on blockchain, Walker decided to test out Voatz in a small pilot project because of her frustrations in making voting more accessible to military and overseas voters. After more than a year of conversations with the startup, she decided to use it in November 2019, for a single issue local special election.

Then, last February, in the wake of the MIT report, West Virginia announced that it would not be using the Voatz app in its state primaries and Colorado then also parted ways with the startup. Three months later, concerned about the negative stories about Voatz, Walker switched, albeit briefly, to a different online voting app for a local election before switching back to Voatz in November for the presidential election. She says she "briefly scanned but did not dissect" either the MIT or Trail of Bits reports prior to her decision and has no conflicts of interest in piloting Voatz.

“We couldn't be happier with how the product worked administratively,” says Walker. “We got comments from our voters who did utilize that product that they really enjoyed the ease of it.” Walker believes Voatz will eventually overcome its security issues and says that process is exactly what pilot projects are for. “It's important for county elections officials, administrators, professionals, to have a seat at the table when not only developing the technology but improving the technology,” Walker says, “and making those necessary improvements to give confidence and integrity in the processes as we move forward.”

Additionally, both Walker and Gardner say they've placed plenty of electoral guardrails around these pilots, including segregating Voatz-cast ballots from the general pool in case vote challenges arise, and giving voters an opt-in to select Voatz or another means of voting.

Still, many information security experts are concerned that the classic startup ethos of monetization through disruption is in complete opposition to the very foundation of elections. “The startup's challenge is to find ways to disrupt the market. The problem is, elections are not a market, they are a public good,” says Tarah Wheeler.

“We don't need to disrupt them. We need to incrementally improve the security while maintaining trust in goods and services. And have we seen what happens when we disrupt elections? Right?!” - Tarah Wheeler

Gardner says despite all the concerns and growing pains, the shift to mobile technology for voting, either through Voatz or some other new mobile voting apps, is inevitable. “In this election, we had people calling in saying, ‘Hi, I just tested positive for COVID. It's Monday. The election date is tomorrow, I can't go. Or what happens if ‘Hi, I'm at the hospital. I had a baby yesterday,’” says Gardner. “Or ‘I was in a car accident yesterday,

I can't make the polling location.' I think the technology now is proven enough and secure enough that we should be able to use it for all these contingencies.”

Whatever the future of mobile voting may be, it's something MacCene Grimmatt will never see come to pass. She died last July in her home at age 107 surrounded by her family and with the peace of mind that she had preserved her nearly century-long perfect voting record—thanks to one determined county election official and a controversial startup that made it happen.