Experts point to red flags that could undermine the nominating process.

By Steven Rosenfeld

The Democratic National Committee may reverse course on its plans to increase participation in 2020 presidential caucus states by offering off-site voting options—starting with telephone voting in Iowa and possibly online voting in other states.

That prospect of a reversal, at least in the early nominating caucuses, stems from growing concerns in top party circles about protecting the “integrity of the process” in a post-2016 climate, said James Roosevelt III, co-chair of the DNC Rules and Bylaws Committee.

“It is entirely possible,” said Roosevelt. “The committee is going to be looking to be convinced that it will work. I think the committee is subject to competing pressures. One is to honor Iowa’s commitment to participatory democracy. And the other is to a heightened sensitivity that did not exist four or certainly eight years ago to the integrity of the process.”

While only a handful of states will use caucuses to nominate presidential candidates, the Democrats’ first contest and third contests are poised to offer an unprecedented remote voting option; by telephone in Iowa, or possibly an online platform in Nevada. Because these are party-run events, government election officials who have been hardening their systems since 2016 against potential hacking—by foreign agents or domestic partisans—will barely be involved. (These officials oversee primary elections, not party caucuses.)

Instead, state Democratic parties will be renting private voting systems that they and voters have not used before. The systems will have registration, balloting, tabulation and auditing components. Security and usability experts who reviewed Iowa’s plans have voiced many concerns about the process. But hovering above their red flags was the dynamic noted by Roosevelt: No matter the caucus night outcome, introducing a new voting system could invite a range of threats that might undermine the nomination.

“No one has formally presented it—but I have heard it,” Roosevelt said, when asked about contentions that the private voting systems could be 2020’s most attractive target for hacking, social media propaganda, and undermining candidates.
(Facebook’s former chief security officer, Alex Stamos, raised that scenario at a Washington press conference on June 10, saying, “Of the 20 candidates, 19 of them have to be losers, right? So that means 19 different populations of people that you can try to convince the system is rigged against them… All you have to do is create a little uncertainty.”)

“As I listen to the general commentary, particularly this past weekend [June 8-9] with all the candidates except Joe Biden being in Iowa, I’m hearing more talk about historical precedents where if someone wins Iowa they are on a glide path” to the nomination, Roosevelt said. “That makes it obviously more valuable [for domestic or foreign meddlers] to create an outcome that may not be accurate.”

The DNC Rules Committee has yet to approve the caucus states’ plans and will meet June 28 in Pittsburgh. Starting with Iowa, state party officials will be asked to respond to procedural and security concerns. The state officials will likely be assisted by vendors who helped to draft a confidential Request for Proposal (RFP) after last winter’s adoption of a delegate selection plan. The Rules Committee will then have to approve each caucus state’s plans.

It is quite possible that the committee will have to evaluate different voting systems in different caucus states. “We’re still in the RFP process. It could end up being over the phone, or as an app, or some other electronic form,” Molly Forgey, Nevada State Democratic Party communications director, wrote in a May 31 email.

**Planning in 2020’s First Caucus States**

The Independent Media Institute’s Voting Booth project obtained a copy of Iowa’s RFP and asked industry and academic experts in remote voting and election cyber-security to assess Iowa’s envisioned telephone-based system. The experts’ top concerns—based on observing similar voting systems used in Canada and abroad, Utah’s Republican caucuses in 2016 and 2018, and in private-sector elections—were, surprisingly, not a reprise of 2016’s Russian hacking. Instead, the experts cited other likely problems that could mar the caucus’s credibility.

Iowa’s RFP, issued May 13, 2019, “seeks experienced, reliable and highly skilled developer(s)/vendor(s) to provide” elements in what is essentially a three-stage process: “1. A virtual caucus platform that can run telephonically. 2. A virtual caucus registration system. 3. A ranked choice voting tabulation system.”
The RFP’s timelines are selecting its vendors by mid-June, have a system ready for testing by October 1, offer virtual caucus registration (only for registered Democrats) from January 6 to January 17, 2020, and offer six telephone sessions between January 29 and February 3. That last night is when caucuses will be held in nearly 1,700 local precincts.

Iowa’s off-site participants must be registered voters and Democratic Party members as of December 31. An additional registration would be required to caucus by phone. That step would involve submitting first and last names, their voter registration address, phone number, email address and day that they plan to vote, the RFP said. They will be asked “at least twice to confirm they intend to sign up for the virtual caucus and acknowledge their understanding… that they will not be able to participate at the precinct caucus.”

After those steps, the voting instructions will arrive. “This may come in the form of an email confirming their registration with a phone number and unique PIN that will allow them to participate in the virtual caucus,” the RFP said. “To ensure the caucuscgoer who signed up for the Virtual Caucus is the person who participates during the Virtual Caucus, a system will need to be developed for two-factor authentication. This information should be something that is not publicly accessible, i.e. last four [digits] of their social security number or drivers license number.”

Voters will call into the system, authenticate themselves, and then hear a series of pre-recorded or live messages where they will then rank their top five presidential choices, the RFP said. The votes must be “stored securely,” and “after the final virtual caucus session, the total results from all six [remote voting] sessions will be combined and then sorted by the participant’s congressional district,” of which there are four in Iowa.

**Experts Cite and Assess Red Flags**

The experts asked to assess Iowa’s RFP mostly cited usability issues as their foremost concern, but also discussed hacking scenarios and issues that could undermine public confidence in the outcome, such as not knowing whether a telephone voter’s choices were accurately counted.

The top red flags concerned potentially thousands of older people having trouble with using a new and unfamiliar telephone system. Specifically, the experts cited voters
having to be authenticated by entering serial numbers on their government ID cards and a PIN sent by email (after registering weeks before), and then having to rank the five top candidates in a lengthy and possibly clumsy process.

“Twenty-three candidates? Do you know how long that will take to listen to have that list read out?” said Aleksander Essex, a cybersecurity and cryptography expert who focuses on telephone and online systems and runs the Western Information Security and Privacy Research Laboratory at Ontario’s Western University. “If you want candidate one, press one... If you want candidate two, press two...’ That’s the problem with telephone voting from a usability perspective, aside from everything else. You have to sit there.”

The “everything else” that Essex and other experts alluded to also begins at the starting line of the remote voting process, such as people other than the voter trying to access and submit their ballots. The concerns continue with cracks in the layers of technology that lie below the surface of any phone, web or app-based interface, and possibly could be exploited. And there’s any accusation, factual or not, that casts doubt on the outcome.

“There is no such thing as unhackable anything,” said Roger Grimes, a cyber-security and penetration tester who has worked for three decades in corporate and military circles, has authored ten books on related subjects, and now trains people to avoid the most common hacks. “Can it be hacked? Yes, it can be hacked,” he said. “But the real expert opinion here is that you’re probably going to have far more usability issues.”

Grimes cited research that focused on one step in the RFP’s envisioned process. Many people simply fail to navigate two-factor authentication, he said—entering information from two different IDs to log in. “But again,” he continued, “If I were a hacker, I’d attack the back end where the data is aggregated. That would be far easier to pull off” than going after large numbers of individual ballots.

Grimes was not alone in saying that human errors and technical hurdles at the start—even if they were not systemic threats—were the top concern that could tarnish 2020’s opening Democratic contest. In Iowa, virtual caucus votes will allocate 10 percent of the delegates to the presidential nominating process’s next stage. This voting bloc could be pivotal in the crowded field with slim margins separating candidates.

“The amount of people who cannot put in a four- or five-digit PIN” is bigger than one assumes, said John Bodin, whose firm Election Trust has run elections for local
governments and non-governmental bodies for two decades. There were many ways for telephone voters to get confused, he said, from being hard of hearing, to hitting a wrong key, to having a call dropped, and then not getting back into the voting system to continue.

“When all those calls [for help] start piling up and they only have 20 operators and they should have 120. That’s what happened in Utah in 2016 [in Republican Party caucuses]. It was a help desk fail. That is what has happened in municipal elections in Ontario,” he said. “Then there’s the authentication piece: Who is actually pushing the send button?”

That last reference—asking whether the person actually voting remotely is the intended voter, or a family member they had passed the phone to, or a campaign worker helping (or pressuring) the voter—is another problem that shadows all forms of remote voting. In 2018, the hijacking of paper absentee ballots in North Carolina’s Ninth U.S. House district led that election to be canceled and rerun. In 2017 in Alberta, Canada, operatives for one candidate hijacked ballots by assisting new citizens to register for their party-run leadership race, but swapped in other email addresses to intercept the voter’s log-in codes and ballots.

Any data system involves risks, Grimes said, but the key is identifying the most likely problems posing real-life impacts, not just theoretical scenarios. Two-thirds of data breaches come from users falling for indiscriminate mass scams, such as so-called phishing, where recipients open links in emails or text messages, and also from not installing software patches, he said. His observation suggested that the universe of off-site voters in any caucus state could be targeted by a range of malicious messages, from disinformation about candidates and voting to attempts to seize ballot credentials.

When told that the most inviting hacking target in 2020 might be privately run early caucuses, Grimes reiterated that hacking into some aspect of a voting system was one thing, but successfully targeting and changing the election results was another—and unlikely.

“This is a highly valuable event, but the likelihood of actual hacking on a level to impact the election is probably quite low,” he said. “It’s difficult to do the hack alone, but it could be done. But it is very difficult to do it in the numbers you would need to impact the outcome of an election. It’d be very difficult for it to occur in a meaningful way.”
This is not to say that hacking pathways and overseas threats are not real, said Essex, whose research has traced voting data as it moves through computer servers located around the globe and has identified security weaknesses in these pathways. But these possible scenarios are eclipsing more basic and immediate concerns, Essex said.

“People are so focused on that [Russian meddling] right now, that they don’t consider the possibility that your election could be undermined by a simple loss of confidence in the process itself,” Essex said. “You actually don’t need Russia to undermine your election. All you need is one candidate who will not concede losing. The system says they lost, but they will not concede. And they are vocal on Twitter. And they have a whole army of people that they can rile up. And they say, ‘Who says we lost? I say we didn’t lose.’”

**Hacking Is Hard, Propaganda Is Easy**

Such demagoguery is not theoretical, Essex said. “This is what we are seeing in Ontario, but kind of a sweet Canadian version of this. But in the U.S., you might see a stronger version. Take that possibility and add the oxygen that a troll army at Russia’s direction throws into the mix [via propaganda placed on social media], and you can seriously get some flames.”

Essex is not alone in voicing such concerns. On June 10 at the Bipartisan Policy Center in Washington, D.C., Nathaniel Persily, a Stanford University constitutional law scholar and co-director of the Stanford Cyber Policy Center, and Stamos, who is now with the Cyber Policy Center, discussed those issues as part of releasing their extensive report on understanding 2016’s Russian hacking and protecting 2020’s elections.

“Where the social media campaigns, the disinformation campaigns, and the election administration issues intersect is on sowing seeds of doubt,” Persily said. “In this environment where we are not trusting our political institutions it becomes very easy to cast doubt on the security of actual elections. Even if the voting machines are working as intended, if you don’t have the kind of auditing and potential paper trail to confirm that everything is working as intended, we are now living in an era where it is very easy to cast doubts on the results.”

Persily and Stamos made many points that could pertain to the 2020 Democratic caucuses, but two stand out. Stamos said most disinformation and propaganda in 2020
would likely to appear to originate from domestic sources. That is because foreign actors—espionage agencies—would be clandestinely “supporting people, and radicalizing groups, and supporting groups that push hard narratives” in the targeted countries, he said. Recent elections in Mexico and India displayed this pattern, Stamos said.

“If I were the Russians, I’d be involved in the Democratic primary right now,” he said. “I’d be trying to build online bases of support for all of the candidates… Not pushing any pro-Russian propaganda; just pushing stuff on behalf of every single candidate, and then building a population of people who I can turn against whoever the eventual nominee is. And then I’d attack the certainty of the election.”

(On Friday, June 14, the European Commission issued a statement saying that foreign-based disinformation seeking to depress voter turnout and sway public opinion had appeared on Facebook, YouTube and Twitter before last month’s European Union elections. Russia was the implied source.)

Persily also noted that the vast majority of social media messages were not fake news or even very political. But apart from silos of deeply engaged partisans, he said that “the most recent studies” found that “old people” were the demographic most likely to see a larger share of online disinformation. Needless to say, this is the same elderly cohort that the other experts predicted would face usability issues when first voting by phone.

The complexities of ensuring a legitimate process do not end there; even verifying vote totals could be challenging, said Bodin. The DNC’s 2020 Delegate Selection Rules require that caucuses have both an audit trail and a process to resolve disputes. The Iowa Party’s Delegate Selection Plan calls for “post-election audits such as manual audits comparing paper records to electronic records.” But Bodin said that so-called hybrid election systems, mixing paper and electronic records, can be hard to reconcile.

“With any hybrid election, that’s the trick,” he said. “It isn’t so much getting it right on electronic or getting it right on paper; it’s getting it right across both platforms. How do you know that people didn’t vote twice?”

Several election experts and insiders expressed concern over the DNC’s initial decision to direct caucus states to offer an off-site voting option as a way to increase participation in 2020. Did the Democrats know what they were getting into?
For example, Iowa’s RFP was six pages, which surprised Essex. “THATS all?” he wrote in an email. “Just for comparison the online voting RFP for Toronto (a mere city) was 180 pages and lays out all kinds of methodology and requirements.”

But Bodin said there’s often a difference between a request for proposal and what gets done. “What the RFP is and what the eventual solution is can be far different… I wouldn’t judge the product from the product description.”

**Next Steps**

Roosevelt, the longtime DNC Rules Committee co-chair, said the panel has pushed aside other business at its June meeting so it can focus on the caucus voting plans—starting with telephone voting in Iowa.

When presented with the potential usability challenges for older voters cited by experts asked to assess the Iowa RFP, he said that list was not surprising. “I wouldn’t say those are the greater concern, but I’d say those were real concerns. We’ll need to hear from them [the state parties and vendors] on how they intend to address them.”

The greater concern, Roosevelt said, was the “integrity of the process.” The Rules Committee will ask caucus state party officials about a spectrum of concerns, he said, and to assess responses before deciding whether or not to approve their off-site voting plans—telephone or online voting.

“It will be the committee’s job to sort through what is propaganda, what is exaggeration,” Roosevelt said, “and then [to decide if it can say] ‘We are satisfied that there are mechanisms in place to guide people through this’ and we’ll take the flack.”

*Steven Rosenfeld is the editor and chief correspondent of* Voting Booth, *a project of the Independent Media Institute. He has reported for National Public Radio, Marketplace, and Christian Science Monitor Radio, as well as a wide range of progressive publications including Salon, AlterNet, the American Prospect, and many others.*