What Iowa Taught Us About Cybersecurity

Andy Liu (HMC '23)

This Sunday night, five full days after results were expected, the controversial Iowa caucuses finally produced a winner, as Pete Buttigieg narrowly edged out Sen. Bernie Sanders in state delegate equivalents. While the results are still subject to change, the public opinion of Iowa as an unmitigated disaster will not. Historic delays, breakdowns in communication, and widely-reported technical difficulties all contributed to a widespread loss of faith in the caucus results that even the candidates themselves have called an embarrassment to Iowans and to the Democratic Party. In the immediate aftermath of the confusion, the Iowa Democratic Party blamed the delay on a broken mobile app developed to tally caucus votes from individual precincts. The app, developed by a little-known D.C. startup called Shadow, became central to a number of conspiracy theories about the fairness of the caucus, especially due to its ties with former Hillary Clinton staffers and the campaign of Iowa victor Pete Buttigieg. What is most problematic about this app, though, is what it indicates about the state of voting security and cybersecurity in the United States.

Cybersecurity concerns surrounding the 2020 Caucus entered the conversation long before Shadow. In fact, in 2019, the Iowa Democratic Party made plans to hold virtual caucuses in order to comply with a DNC mandate to improve accessibility, but these plans were eventually rejected by the DNC, who cited cybersecurity concerns in doing so. Analysts have suggested that caucuses are much more easily virtualized compared to primaries, as caucus results do not need to anonymize individuals' votes. However, the cybersecurity community resoundingly praised the DNC's decision. Virtual caucuses have long failed to hold up under scrutiny, with cybersecurity experts breaching many potential systems and raising the threat of denial-of-service attacks or foreign exploitation. As a result, Iowa replaced their proposed virtual caucuses with a series of "satellite caucuses".

However, this was not enough to remove all cybersecurity concerns from the caucus, which faced a plethora of issues. The caucus app itself raised a number of issues for leading cybersecurity experts. While the most dangerous issue - the potential for an outside hacker to hack into the app and change election results - is virtually impossible in a caucus (as each precinct will have paper records showing the true results even in the event of an attack),

experts still warned of a number of other issues, including denial of service attacks that could take the app down and cause significant delays.

These issues would be raised about any app, but the way the Iowa Democratic Party chose to use the one developed by Shadow made the voting process of this year's caucus especially suspicious. Shadow itself is a small, unproven tech startup whose parent company, Acronym, is led by a controversial party operative. The app was distributed through TestFairy, a mobile app development platform meant for app testing but not official app distribution. This suggests that the app did not meet the stringent security and performance requirements of the App Store or Google Play. This strange choice of platform meant that precinct captains were forced to undergo a confusing "sideloading" process to get the app on their devices, which was exacerbated by the difficulty of logging in.

Most concerningly, the Iowa Democratic Party refused an offer from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to help test the app. Additionally, they strayed from best cybersecurity practice in other key areas - the app appears to have been rapidly developed even in the days leading up to the caucus, and testing was intentionally delayed to keep the app from "potential hackers". App testing CEO Dan McFall noted as such when asked about the Iowa caucus: "It's a tale that we have seen with our enterprise customers for years: A new application was pushed hard to a specific high profile deadline. Mobility is much harder than people realize, so initial release was likely delayed, and to make the deadline, they cut the process of comprehensive testing and then chaos ensues."

When viewed from this angle, it almost seems unsurprising that such an app would fail the test of the Iowa caucuses. And, indeed, on the night of February 3, the app failed consistently across all precincts, preventing precinct captains, many of which were insufficiently trained on how to use the app, from reporting results. When precinct captains turned to the backup plan - directly reporting results to the Iowa Democratic Party headquarters via phone, the phone lines quickly became clogged - partly due to the efforts of internet trolls who found the publicly-available number flooded it with hostile calls. As a result, both the primary and backup results-reporting systems were quickly brought to their knees,

and the first results - which themselves were riddled with inconsistencies - were not reported until the next day.

So, now over a week since the Iowa caucuses, what lessons can we learn from the chaos of February 3, 2020? While the worst-case scenario - outside manipulation of the voting results - has thankfully been avoided, the impact of technology on the caucus remains undeniably negative. The secrecy surrounding the app and its development process - despite offers for testing from reliable outside sources that would have helped strengthen the app's security - reflects the fundamentally flawed philosophy of "security through obscurity", which aims to create a secure app through secrecy rather than actually creating a secure app.

Additionally, the lack of cybersecurity expertise displayed by the IDP and by Shadow indicates a need for political organizations to truly understand the nuts and bolts behind the technology they use. While technology can absolutely help with politics, it always comes with added risks. The failure of the IDP to recognize that, instead of relying on a hastily developed, insufficiently tested and potentially vulnerable app to report results, casts grave doubts on states' current ability to introduce more tech into the voting.