The Future of Voter Confidence: Voting in a Post-Pandemic World

While much of the world as we know it has changed since the COVID-19 outbreak identified in 2020, one of the very few things that has remained steadfast is an appreciation of voting. If anything, it could be argued that voting is even more important today, as governing bodies and society as a whole seek to establish consensus on countless, often contentious, issues now seen through a post-pandemic lens.

The importance of voting has not changed, but the *way* people vote has. Living in this new world demands safe, accurate, responsible options for voting that consider everything right down to the carbon footprint . Although people want to vote, preserving voter participation and confidence today will require fresh thinking and entirely new options.

The purpose of this paper is to examine systems for voting and decision making wherever they take place today. It could apply to leadership in a homeowners association (HOA), a private club or union, a corporate board of directors, or to elected officials in government at any level. The principles are the same.

No matter what the governing body though, obstacles to successful elections in the current environment include:

- Physiological/Viral (medical risk)
- Psychological (fear of infection and confidence in the process)
- Technological (voting accuracy)

Data suggests a correlation between infection rates and physical voting. Specifically, a study published by NIH and the University of Wisconsin examining infection rates at the county level after the presidential election primaries of April 7, 2020 found a 10% increase in in-person voters per polling location associated with an 18.4% increase in the COVID-19 positive test rate 2–3 weeks later.
Emerging queueing theory will help determine future guidelines for in-person voting, but it's clear there is a multitude of dimensions to consider regardless of whether voting is in the private or public sectors.

Voting is evolving.

Voters can be fearless. We've seen that repeatedly across the globe where individuals are willing to vote even at tremendous personal risk for their safety. Voting seems to satisfy an innate need to be heard and to make a difference.

At odds with this is the desire to be safe in a post-pandemic world. Online voting seems to address both concerns. There is every reason to think that online voting is here to stay. Certainly its minimal environmental impact compared to on-site voting is an advantage today. Furthermore, online voting helps voters faced with mobility issues, including the elderly, the disabled, and people suffering from ambulatory injuries.

These factors, in combination with the lasting psychological effects of the pandemic, tell us that hybrid voting environments that combine online, mail and in-person voting are likely to stay regardless of the persistence of any virus. Voters will increasingly expect a remote option given its appeal in terms of safety, carbon footprint, and overall access.

As a hybrid choice proliferates, the issue of voter confidence in any new system will, to some degree, be minimized through the growing confidence that comes with widespread adoption of new technology. Sheer repetition engenders trust, to some degree. Moreover, in our increasingly digital world, cybersecurity countermeasures continually proliferate.

Nonetheless, voter confidence is also fragile. It must always be a consideration because of a growing diversity of vendors and a lack of standards across platforms. Voting is still a "Wild West" free-for-all full of tech marvels, but also platforms built on questionable or dated technology. Risk pervades the industry. Branding will, therefore, be an essential part of establishing and securing ongoing trust in particular systems owing to the inherent leap of faith between voter and governing body. Stakeholders participate in a system where they essentially surrender trust to a mysterious black box. Moreover, this black box can have a direct impact on some of the most significant assets held by any household, including real estate property values, potential rental income, and any related rights possessed by stakeholders.

Voting platforms vary wildly.

It is important to distinguish any proprietary elements to a particular voting platform because any loss of confidence in one system should not be allowed to erode confidence in the entire process. There is still significant downside risk for the category. Anyone holding an election should be able to show they value election integrity enough to choose a highly qualified partner. Any scenario where trust is given to a black box, then compromised, risks an erosion of trust. Consequently, safeguards must be in place to anticipate and manage reputational risk and any damaging misconceptions. In the case of voting platforms, those safeguards would be some degree of understanding of industry standards and best practices. In other words, the brand of a particular voting platform must stand for something to set itself apart from competitors. For many reasons, voting platforms must not be seen as parity.

The voting platforms that will win the day will not only be the best engineered, but also the most clearly defined as a brand.

As voting evolves, election integrity will take the spotlight.

Safety is the white-knuckle issue of the moment. This means physically minimizing the risk of infection from other in-person voters who are in the queue to vote in public and private elections . At issue is protecting the voters, but also the individuals on-site overseeing the process.

Given these concerns, online voting stands to proliferate, though not without raising the specter of its own set of security issues. Poll after poll shows that the majority of people still do not trust online voting. They fear interference that can taint results at a number of points of vulnerability throughout the process.

This much is clear: The rise of online voting puts the issue of election integrity into full view.

Integrity can be engineered into the election process.

Maintaining the integrity of an election is both an engineering challenge and a communications challenge. You want to integrate unbreakable elements such as end-to-end verification that protects the vote, but you also need people to gain confidence in the system and its outcome by grasping the value of these measures. Neither is easy. Software engineering is esoteric, complex, and fast-moving. It may also be subject to bad actors, so security is effectively a moving target. Overcoming these issues raises its own set of challenges to the tech world, but are just as challenging to explain to the layman.

One answer to maintaining voter integrity is through robust data encryption. Encryption is integral to how people bank online, send email and text messages, and engage in e-commerce. It's effective and trusted.

Encryption works, but at some point you have to decrypt. And therein lies the problem. Voting data is not static, so the integrity of the data must be protected at every single layer before, during and even after the online vote is cast. Unencrypted voting data is not immutable. Every time data is unencrypted to, for example, accept a vote, you introduce vulnerability. Add personal computers at home where many will likely be voting, and you have even more threats to consider.

Homomorphic encryption

It is possible to perform calculations and computations on encrypted data without first decrypting it. There is a way for votes to be added together, counted, tallied, verified, and even audited—all without decrypting. These are some of the privacy-preserving characteristics to homomorphic encryption. Encrypted votes stay encrypted, so you can aggregate them in encrypted form and decrypt them once you have a full record of how many votes were cast for each candidate. All the while, you've protected the anonymity of each ballot while preserving end-to-end verifiability.

Using homomorphic encryption, individuals can independently confirm their vote was counted and not altered. Similarly, third parties can build auditing capabilities that allow them to confirm that votes were properly tabulated.

Systems can be implemented with varying degrees of homomorphic encryption, but full homomorphic encryption (FHE) is ideal for online voting solutions, particularly when they're in the cloud.

SUMMARY

Voting is more important than ever, but safety and security concerns in a post-COVID world make online voting an increasingly popular option that is unlikely to go away. While online voting is undoubtedly more convenient, it raises its own issues of security and trust. One solution to ensuring voter integrity is through the use of full homomorphic encryption. Homomorphic encryption is a powerful tool that enables you to compute on data while the data remains encrypted, thus preserving the vote as intended while also allowing for end-to-end verifiability for all stakeholders.

Author: Tom Thomas

Tom is the co-founder of Votegrity. He has more than 25 years of experience in Information Systems, building high performing engineering teams. During his career, he has spent time designing, building, deploying, and maintaining customer-focused, data-driven enterprise applications and systems in organizations ranging from startups to Fortune 50 companies. He holds an Executive MBA from Seattle University and a Bachelor of Science in Software Development.