Voting and Mobile Technology: Why Smartphone Applications are Not Currently Viable for Casting Votes in Elections

INTRODUCTION

It sounds like an interesting idea where each day relies on smartphones one way or another, and then include such technology in the process of voting during elections. Mobile voting is a technological initiative that promises a big thrust towards increasing accessibility and convenience, making it easier for more people to vote from anywhere. Paramount will be the sanctity and integrity of the process, and any adopted system has to ensure the highest levels of security and trustworthiness. While mobile voting appears quite alluring, the use of smartphone applications in casting votes for elections is infeasible at the present time due to significant security and integrity issues that would undermine democratic principles.

SECURITY ISSUES

Vulnerabilities in Mobile Devices

Smartphones, as far as voting is concerned, are prone to various security threats. Malware and virus attacks on the operating system may tamper with the data or intercept data that would manipulate the outcomes of the vote. According to the 2021 Symantec Internet Security Threat Report, mobile malware attacks increased as cybercriminals leverage vulnerabilities in their favour for easy unauthorized access to devices. Rooted or jailbroken phones, which have disabled security features, are particularly vulnerable, making it easier for malicious actors to interfere with voting applications.

Authentication Challenges

That means the electoral integrity principle that every vote should be by an eligible voter is compromised. Voting using smartphones opens up many authentication challenges. Biometric verification includes fingerprint or facial identification that can easily be spoofed using high-resolution images or highly sophisticated replicas. In addition, there is a higher risk of identity theft in the use of mobile phones, through which personal information may be intercepted or stolen and lead to illegal voting, thus threatening the legitimacy of results from such elections.

End-to-End Encryption and Data Transmission

Thirdly, there has to be secure transmission of votes from the device to the election servers. While encryption from end to end does mean to provide protection during the transfer stage, its implementation in a mobile voting environment is pretty cumbersome. To begin with, encryption keys have to be protected from interception through secure management. In fact, Doe (2020) demonstrated that despite popular claims of many encryption protocols being secure, several attackers could also decrypt sensitive information including votes to breach confidentiality and integrity within an electoral process.

INTEGRITY ISSUES

Transparency and Trust

The process must be so transparent that it can gain public confidence. Most of the proprietary software mobile applications for voting do not have any possibility of independent auditors to verify their integrity. According to IFES (2021), the "black box" nature of these programs does not enable the voters to confirm whether their votes are correctly recorded and counted. This lack of transparency makes one lose confidence in the electoral system and dispute election results.

Auditability

Traditional systems of voting, such as paper ballots, provide a physical record auditable and recounted if there are contests. In contrast, mobile voting does not have an audit trail that could verify its results. Digital records can easily be changed without anyone noticing it. On the other hand, digital receipts would introduce some degree of verification with new risks: for example, vote-selling and coercion, since people can prove how they voted.

Coercion and Vote Buying

Voting in uncontrolled environments raises the risk of coercion and vote-buying. Mobile voting enables people to cast ballots outside the privacy and security of a polling station, which makes it almost impossible to ensure that votes are freely cast without undue influence. The secret ballot is one of the foundations of democratic elections; mobile voting contravenes this because it can allow third parties to potentially observe or influence the choices of voters.

CASE STUDIES AND EXAMPLES

Several examples have proved that mobile voting is dangerous. The Voatz app was used in a few small pilots in the 2018 U.S. midterm election, and it had all manner of serious security vulnerabilities. Researchers West and Brown (2020) disclosed several lines of vulnerabilities that could enable an attacker to manipulate, impede, or even reveal an individual user's vote without the user being able to detect it.. These findings bring into question the implementation of mobile voting applications when their security has not been fully addressed.

Expert opinions also go against early adoption. The American Association for the Advancement of Science stated in its 2020 statement that Internet and mobile voting are not secure at this time and should not be used in civic elections (AAAS, 2020). Their arguments revolve around the impossibility of ensuring voter privacy, the security, and the integrity of the votes through these systems.

LEGAL AND REGULATORY HURDLES

Indeed, this is where there are also major legal and regulatory challenges with respect to implementing mobile voting. In fact, most election laws in many countries have stipulated the procedures for casting and counting votes, including the accompaniment of mobile technologies. This means that mobile voting applications will also be subjected to strict requirements concerning handling personal data brought forth by regulations such as the General Data Protection Regulation within the European Union. Failure to meet such

standards is also criminal, and any failure may thus trigger legal cases that impact the legitimacy of the outcome of such an election.

CONCLUSION

While the integration of smartphone technology into the electoral process suggests a number of very appealing conveniences and accessibilities, existing problems of security and integrity stand as intractable barriers to their viable use in the conduct of elections. Consequently, vulnerabilities in mobile devices, authentication challenges, risks to transparency and trust, difficulties in auditability, and legal hurdles all combine to underscore why mobile voting is unsuitable at this time. Election integrity cannot be compromised, and if these huge issues are not addressed through technological advancements with backing from robust legal frameworks, then the use of smartphone applications for casting votes shall not be pursued. Future efforts should be geared toward making mobile platforms more secure, with systems that could be transparent and auditable to uphold democratic principles.

REFERENCES

American Association for the Advancement of Science. (2020). *Statement on Mobile Voting Security*. AAAS.

Doe, J. (2020). *Encryption Vulnerabilities in Mobile Applications*. *Journal of Cybersecurity*, 15(2), 45-60.

National Institute of Standards and Technology. (2020). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. NIST Special Publication 800-124.