OSET INSTITUTE

Election Policy Briefing

Will We Ever Vote on Our Phones?

Some Straight Answers

Prepared For:
Public Policy Leadership & Interested Citizens

Prepared By:
E. John Sebes
Co-Founder & Chief Technology Officer

Release Date: 20 October 2020

Here is a very important question: "*Will we ever vote on our phones*?" We see it asked more and more; and now with the 2020 election season racing toward conclusion, there is a fevered pitch to the tone of the ask. But the thing is, it's also not the right question.

The right question is "*Will we ever vote on our phones, safely and legally*?" Today some Americans do vote on their phones, with simple apps or web interfaces that are *not* safe and do *not* try to truly address the many cyber security problems of using the Internet to perform a vitally important transaction that's subject to fraud and theft, and *cannot* be undone.

Moreover, today's approaches (that do not qualify as "solutions") also have some significant legal issues, both rights issues like equal access and equal protection, and election law issues such as conforming to legally required practices for election administration. For both reasons, today's approaches also create the opportunity for legal disputes that can undermine public confidence in election results.

So: "*Will we ever vote on our phones, safely and legally*?" Here's the short answer: **yes** (*but*) only when both of two critical transformations have been accomplished.

1. Mobile voting needs to become the exact digital equivalent of paper based home voting, with an actual ballot, and with election officials completely in charge of voter identification and of decisions about whether ballots are to be counted.
2. This "digital remote voting" process needs to be implemented with some specific cyber-security protections that are not available today, but could be put in place if computer science R&D shows practical solutions to six (6) hard problems in cyber-security.

Let's start with legal and procedural issues, and then shift to safety issues about the technology that's required to protect the digital voting process.

The Transformation to Digital Remote Voting

Many of the attempts at Internet voting (or the minor variant of mobile voting) using a personal computing device like a phone or tablet, have not even attempted to be legitimate "ballot marking and return." Instead, the user sees web forms or mobile app screens where they can

make ballot selections that are recorded locally, transmitted over the Internet, and recorded in a database somewhere. There isn't actually a ballot. One other item that's lacking: any way for an election official to determine who the voter is, and whether to count the ballot. Instead, the vendors and operators of mobile voting systems are the ones who decide who is allowed to vote, sometimes based on the user's presentation of a PIN (personal identification number delivered by postal service or eMail, and easily misappropriated to enable voting fraud), or occasionally through more exotic attempts at "authentication" such as asking the user to take a phone selfie to be compared by software to some other image on file.

In any case, what's most notably missed is an election official (EO), executing their duty to make best efforts to identify the voter, and determine whether the ballot is to be counted. Instead, there is software taking the place of the EO, networks and database taking the place of a ballot, and no real indication of the voter's identity.

That's not actual legal voting in most U.S. states.

If we are to someday "vote on our phones" the voting process needs to ***exactly*** follow the existing process of paper-based remote voting, also known as "absentee voting" or "vote by mail," or "vote at home." That critically includes the technology for election officials to perform, and to be in control of, the digital versions of the existing processes for ballot intake, adjudication, and counting. And ***that*** will require some changes in cybersecurity technology as described in the next section.

2. The Transformation to Digital Remote Voting with Security

It's very likely that in the future it will be possible to create a mobile voting system with many more technical safeguards than today's systems. However, getting there will require technology to develop solutions to at least six (6) security issues. Each of those issues requires a solution to one or more hard problems in computer science. There is certainly relevant work in progress, but today, no one has shown how to solve these problems. Let's consider each of them without having to delve to technically deep for the sake of the reader.

1. **Endpoint/Device Security**: Today, a voter uses a device (e.g., PCs, tablets, phones) that is subject to malicious software attacks via the Internet from anywhere on the planet. To make digital ballot protection roughly on par with physical ballot protection, we need a device with new security technology that can ensure that its software and data is not tampered with by malicious software. Currently, there is no such technology for most devices, including consumer mobile devices.
2. **Strong Voter Authentication**: What is required is a method of digital authentication of voters by election officials that:
    a. preserves ballot anonymity;
    b. is feasible for use by ordinary voters and ordinary local election officials;
    c. with digital identity infrastructure controlled by state or local election officials (not 3rd parties or vendors);
    d. just as they are currently in control of the process of identification of the voter of each paper by-mail ballot.

Current digital signature techniques are not easily usable, and require costly infrastructure that most state and local election officials would not find feasible to deploy and administer.

3. **Anonymous Ballot Marking**: Mobile voting requires techniques for a voter to use their device to obtain their proper ballot based on their voter registration, and then to vote that ballot, in a manner where the voter's identity and ballot selections are *not* able to be viewed at the same time by any part of the mobile voting system. Existing technologies permit *both* identity and votes to be present at the *same* time.
4. **Ballot Transport Security**: Mobile voting requires a method for delivering a digital remote-ballot "kit" (i.e., ballot, shielded from view, combined with voter identity information and digital authentication) from a voter's mobile device to a digital "drop box" system, where the voter is protected from a wide variety of current threats to:
   a. transport security (malicious-actor-in-the-middle (MITM) attacks, spoofing and others);
   b. reliability; and
   c. known-delivery assurance.

   General solutions to these Internet security problems just are not currently available.
5. **Ballot Box Security and Chain of Custody**: digital ballot return requires sending ballot kits to a destination ("target") system. That system needs to be connected to the Internet, serving as a gateway to a repository of digitally returned ballots. That target system, as well as the ballot-kit repository, need security technology that can ensure that both the system's software, and ballot data *cannot* be tampered with by malicious software, and that returned ballot kits are accessible by authorized individuals. Such a system must be under the administrative control of election officials, not I.T. administrator staff that could abuse admin privileges to tamper with the system or the ballots. Technology for such tamper-proof Internet-connected systems does *not* exist today.
6. **Auditable Digital Ballot Processing**: election officials require another malware-proof system that is under their control in order to extract the digital ballots from the digital ballot box, and to perform the digital equivalent of absentee ballot authentication, adjudication, and submission to the counting process. However, that digital remote-ballot process also needs to include a method for end-to-end audit, to ensure that the digital ballot submitted to the counting process is, in fact, the exact same ballot that the voter submitted. Some end-to-end audit technology exists, but it requires integration with several of the above currently-non-existent technologies, and must be proven to be usable by voters and election officials.

The first three of these required solution components—each requiring a solution to one or more hard problems in computer science—are required to implement a digital ballot marking and return process with the same constraints and controls as found in current legally authorized paper remote voting.

The last three of these required solution components each first need solutions to hard technical problems in order to comply with an important legal requirement of U.S. elections: the process and its results are the responsibility of a *trusted central election authority*, typically a local elections office or commission. This is simply a matter of current states' election laws, regardless of the academically engaging discussions about central vs. decentralized authorities.

Some or all of these may seem to be daunting challenges. Yet, in most of them there is plenty of existing technology already in use, or now in development, that can meet the needs. However, neither security technologists nor election technologists have the mission to extend and integrate existing work specifically for the needs of elections. If that can change, then work in the six areas could move us substantially closer to safe, legal mobile voting.

In a longer version of this Briefing, I provide more details on issues of the first transformation, as well as a more detailed examination of each of these six component requirements: both to explain and illustrate why it is necessary for digital remote voting to be ***equally*** protected as paper based remote voting, and to provide a prospectus on the achievement of these technical challenges.

About the Author

John Sebes is one of two co-founders and Chief Technology Officer ("CTO") for the U.S. based **OSET Institute** (“OSET”), a non-partisan non-profit 501.c.3 public benefit corporation headquartered in the Silicon Valley. He leads all aspects of technology strategy, vision, architecture, engineering and development for the TrustTheVote Project – the flagship effort of the Institute.

Prior to founding the OSET Institute, John has been a software engineer, technical consultant, and CTO, working in several areas, including network infrastructure, application frameworks, embedded systems, critical infrastructure, data center operations, with strong common themes of risk management, security, privacy, and reliability. Innovation and technology transfer have been another consistent theme, in settings as varied as government-funded R&D, venture-backed start-ups, professional services, academia, and non-profits.

For parts of his career, John provided independent consulting services related to information security and IT operations assurance, for a variety of organizations ranging from technology start-ups and venture capital firms to major government agencies and established financial services firms. At other times, John has been a Principal Investigator in R&D projects, ranging from DARPA projects performed in the pre-Web era, to recent work with DHS on public (open source) security technology.

Previously CTO at Solidcore Systems, Inc.; VP Strategy at Securify; Technology Officer of Network Associates Labs; and variety of consulting, development, and R&D management roles at commercial InfoSec pioneer Trusted Information Systems.

John is a co-author of 12 patents and 20+ publications.

About the OSET Institute

The Open Source Election Technology (“OSET”) Institute, fiunded in 2006, is a 501(c)(3) tax-exempt nonpartisan, nonprofit election technology research corporation chartered with research, development, and education in election technology innovation in order to increase confidence in elections and their outcomes in defense of democracies, as a matter of national security.

The Institute’s flagship initiative, the TrustTheVote Project is a democracy software foundry that is building **Elect**OS, a next generation higher integrity, lower cost, easier to use election administration and voting technology framework freely available for any election jurisdiction to adopt, and have professionally adapted and deployed. ElectOS and all open source election technology is being designed and engineered per the requirements and specifications of election officials, administrators, and operators through a Request For Comment (RFC) process.

As part of our research, development and education mission, from time to time, the Institute produces technology policy research briefings and other related policy content to inform stakeholders, supporters, and the public about issues of election technology innovation and integrity, as well as innovations in election administration process.

Threats to free and fair elections anywhere are inherently threats to our democracy everywhere