FREE SPEECH FOR PEOPLE .ORG

Misleading claims from Bradley Tusk and Mobile Voting Project

The system developed and offered by Mobile Voting Project (MVP), VoteSecure, is *not* a functioning mobile voting application or system. It is a cryptographic protocol that can be integrated with a mobile voting app. It cannot be used without a commercial, non-open source, internet voting system or mobile voting app committing to integrate VoteSecure, and any jurisdiction would need to procure that voting system.

Tusk and MVP developed a product, VoteSecure, and have promoted it as a free, open-source mobile voting application, but this is profoundly misleading.

On its website, MVP describes in detail the process of accessing, marking and returning a ballot, claiming that this is how the "*technology we have developed works*." In various media, talks, and podcast appearances, Tusk has claimed he was demonstrating VoteSecure, as he walked his audience through the steps to access a ballot on his phone, mark it and return it. The representation is false as VoteSecure can do none of those things.

VoteSecure is a cryptographic protocol that may be integrated with a mobile or internet voting system to offer verifiability, but it will not record or transmit votes without a commercial, non-open source voting system.

The VoteSecure developers have made this plain on their website, which states VoteSecure is *"not a complete voting system."*

This has not hampered Mr. Tusk or MVP's representatives from promising that it has developed a product will allow people to vote on their phones, misleading lawmakers, officials and stakeholders to think he is offering a free, open source mobile voting app.

Mobile Voting Project's system will not be used in Anchorage, Alaska.

Tusk and MVP secured a front-page *New York Times* story promoting mobile voting that relied on the false claim that Anchorage, Alaska would soon be using MVP's VoteSecure.

The story prompted the city clerk to issue a press release disavowing the story. Tusk continued to repeat this falsehood in the press and on podcasts causing Anchorage to issue a cease and desist letter in an attempt to stop Tusk's false claims.

Printing paper ballots after transmission, and "air-gapping" the tabulation device does not mitigate the security risks inherent with mobile voting.

Tusk and MVP have incorrectly asserted that cyber-attacks can be effectively mitigated if the electronic ballot is printed on paper after it is received at the election office and the tabulation is conducted offline.

Any cyber-attack, or manipulation of electronically transmitted ballots, can occur *after* the voter reviews the ballot, and *before* the ballot reaches the election office for printing. This means the printed ballot would reflect the corrupted votes chosen by the attacker, not the voter. Printing a ballot transmitted over the internet does not protect it from online threats.