Towards Thwarting Vote-Buying in Random-Sample Elections

INTRODUCTION

So-called “improper influence” in elections may be defined generally as the illicit at least attempted changing of the voting behavior of an individual voter, typically by “vote buying” or “coercion.” Random-Sample Elections take a novel approach to protecting against improper influence. They appear to have the potential to protect against it better than even the best practices in conventional mass elections (even though there may be solutions for polling-place voting, such as those Scantegrity demonstrated in 2009). Moreover, the various trends towards increased remote voting in conventional elections is tending to make them significantly more vulnerable to improper influence. Improper influence not only gives unfair advantage to those with resources to violate the integrity of elections, but it produces victims and contributes to erosion of public trust in such elections. The erosion of confidence in elections is a vicious cycle, since it may in turn reduce participation, which may even further erode confidence.

Improper influence is apparently facilitated when votes can be cast without the protections offered by polling places, at least for mass elections. Random-sample elections may appear to be disadvantaged in preventing improper influence because they do not involve polling places; however, the surprising key to their ability to thwart improper influence is a fundamental difference with mass elections—that nobody need know which individuals have been selected to vote.

MORE ON THE PROBLEM

Vote buying and coercion often go hand in hand. In certain parts of the United States, for example, vote buying with a coercive element is a well-established practice, even for polling place elections. One example is so-called “chain voting,” in which voters are supplied a marked ballot before entering the polling place and must return an unmarked ballot when leaving in order to obtain payment and/or avoid retribution. Small particles on particular levers of lever machines are reportedly used to reveal which levers a voter has pulled to someone inspecting the booth after the voter votes. Lever machines have other “tells” observable in the polling place, such as by removed back covers or the differences in the sound of different levers. Electronic voting machines used in the Netherlands and some other European countries were found to offer such features by radio emanations. Electronic voting machines used in all Brazilian and Indian elections, as well as many US jurisdictions, allow a poll-worker to remotely see and control the state of the machine in the booth at all times, thereby facilitating the technique of leaving the machine in a state where the previous vote is visible to the next voter. In a related apparent scare tactic in all Brazilian voting, which is being spread to other Latin American countries, voters witness their own unique voter identification number, and increasingly even their fingerprint, being provided to the same machine that they are then to cast their vote on, creating uncertainty as to whether their identity and vote are stored together.

Vote by mail, whether mandated for rural citizens or everyone in a growing number of states in the US, including Washington and Oregon, opted for by increasingly permissive laws in many other states, or a available to those voting from outside the country, makes improper influence even easier in mass elections than with polling-place voting. One well-know type of scheme is where groups, such as churches or various clubs, “assist” their voters in filling out ballots received by mail in large sessions. Another is husband and wife filling ballots together. Remote voting from outside a country, called “external” voting, often involves military voters and such voters have often only been able to vote by exposing their choices to those in command, such as by using military facilities to submit ballots by fax.

Ballots sent by mail in whatever context, after in-person purchase by a vote buyer, can be filled and safely mailed anonymously by the voter buyer. When votes are submitted online, however, the vote buyer can be even harder to entrap or prosecute, since no in person purchase is required. For example, a voter could simply make a video of the voting act, including capturing themselves and the relevant screen, and make this available to the vote buyer online. The buyer might even be operating from abroad and use readily-available techniques to hide his or her location or identity.

RANDOM-SAMPLE SOLUTIONS

In random-sample elections, coercion becomes much more difficult if not impossible. The reason derives from a potential coercer not knowing who has received a ballot, the fundamental difference already mentioned. Unlike mass elections, where everyone will be able to vote, only a very small fraction of the population votes in any particular random-sample election. So a coercer may approach people, but even voters can likely vote discretely and simply deny that they were selected to vote. This leaves the problem of vote-buying.

Random sample elections only accept votes online, using codes that voters take from a printed form, which might appear to make them more vulnerable to vote buying as also mentioned above. A new technique, however, may be able to turn this around and allow such elections to provide superior protection against vote buying. The concept proposed in the Random-Sample Elections white paper is based on the technique of what are called “fake” ballots, ballots whose votes will not be counted. These fake ballots should be essentially impossible to distinguish as such, whether by inspection or even in light of what becomes public through auditing after the election, and so will appear to a vote buyer as potentially valid ballots. The idea is essentially to flood the market with such fake ballots. The price for votes offered by vote buyers would ideally be driven down by such flooding to a level that is insufficient to corrupt voters. There are a variety of ways that fake ballots can be made available.

One approach to distributing fake ballots is for those running the election to simply sell them to any entrepreneurial party. The price at which the fake ballots would be issued to such entrepreneurs should preferably be set low enough, such as close to the cost of production, that offers from real buyers at such prices would not significantly corrupt many actual voters. Since the identity of voters are not revealed, at least during the election (some variations go further and even protect it in perpetuity), vote buyers would presumably be forced to make their offers to buy known to large numbers of potential voters in order to reach even a small number of actual voters. And when an entrepreneur finds such offers that are significantly higher than the issue price, the entrepreneur would simply purchase fake ballots from the election authority at the issue price and then try to resell them at the higher price to the vote buyer.

A second but only slightly different approach to distributing fake ballots, that outlined in the white paper, is to provide any number of them for free up to a certain point before the election. It seems reasonable to assume that in a kind of “steady state” arrived at during a process involving many even overlapping elections over time, that this approach may be essentially equivalent to the first approach mentioned above, as the number of fake ballots potentially needed would in most cases be known in advance. If, however, in the exceptional instance the total number of fake ballots for which provisions had been made in setting up the election proves insufficient, the election could potentially be re-run.

A third approach entails providing fake ballots to randomly selected voters. These voters would also be provided with a disposable “proof” that the ballot is in fact fake. Such a proof would be just a digital cryptographic key, provided via another channel to the recipient of the fake ballot. The protocol in the white paper can be adapted to accomplish this. An advantage of this approach is that it would make getting ahold of all the fake ballots very difficult for an improper influencer. This approach could of course be run in parallel with the first or second approach outlined above.