# Coercion

In designing this system, we made explicit decisions regarding how much to complicate the protocol and impede the voter experience in order to mitigate known coercion threats. Specifically, one known threat is that a voter is instructed to create a ballot in a particular way but to then execute a decision to cast or spoil the ballot according to stimulus received after the ballot has been completed and the receipt has been generated. The stimulus could come, for example, from subtle motions by a coercer in the poll site, the vibration of a cell phone in silent mode, or some of the (unpredictable) data that is printed on the voter’s receipt. Some prior protocols have required that the receipt, although committed to by the voting device, not be visible to the voter until after a cast or spoil decision has been made (perhaps by printing the receipt face down behind a glass barrier) and configuring poll sites so that voters cannot see or be seen by members of the public until after they have completed all steps. We could insist on similar measures here, but in an era where cell phones with video recording capabilities are ubiquitous and eyeglasses with embedded video cameras can easily be purchased, it seems unwise to add complications (such as privacy sleeves) which mitigate some coercion threats but leave others unaddressed.

A similar threat of “chain voting” is possible with this system wherein a voter early in the day is instructed to neither cast nor spoil a ballot but to instead leave the poll site with a printed ballot completed in a specified way. This completed ballot is delivered to a coercer who will then give this ballot to the next voter with instructions to cast the ballot and return with a new printed ballot – again completed as specified. Chain voting can be mitigated by instituting time-outs which automatically spoil ballots that have not been cast within a fixed period after their production and by attempting to prevent voters from leaving poll sites with printed ballots, but, beyond simple mitigations, we take no extraordinary steps to make chain voting impossible.

Measures are taken to avoid introducing new means of coercion. For instance, the required identifiers on printed ballots are dissociated from take-home receipts by not including any publically-linkable data. Thus, even if complete copies of all paper ballots are made public, there will be no loss of privacy or coercion opportunities introduced.

# Absentee and Provisional Ballots

There are several methods available for incorporating ballots which are not cast within the STAR-Vote system – such as absentee and provisional ballots. The simplest approach is to completely segregate votes and tallies, but this has several disadvantages – including a reduction in voter privacy and much lower assurance of the accuracy of the combined tally.

It may be possible to eliminate all “external” votes by providing electronic means for capturing provisional and remote ballots. However, for the initial design of the STAR-Vote system, we have chosen to avoid this complexity. Instead, we ask that voting officials receive external votes and enter them into the STAR-Vote system as a proxy for voters. While this eliminates the ability of external voters to explicitly audit their own ballots, the privacy-preserving risk-limiting audit step is still able to detect any substantive deviations between the paper records of external voters and their electronically recorded ballots. This provides high assurance in the veracity of the election tally without reducing voter privacy.