

# Election Verifiability



Josh Benaloh  
Microsoft Research

## Paper versus Paperless

Paper is *not* a requirement.

Availability/Survivability is a requirement.

Integrity is a requirement.

Privacy is a requirement.

Accessibility is a requirement.

Manageability is a requirement.

Paper is a medium ... a detail.

## Requirements

- **Requiring paper makes no sense.**

*Paper is a very poor proxy for integrity.*

- There are paper-based systems with low integrity.
- There are paperless systems with high integrity.

- **Requiring no paper makes no sense.**

*There are many possible uses for paper.*

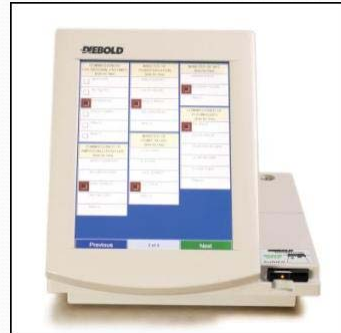
- Lack of paper can add complexity.
- Use of paper can improve manageability.

## Two Sample Systems

- Enhanced DRE
- Enhanced OpScan

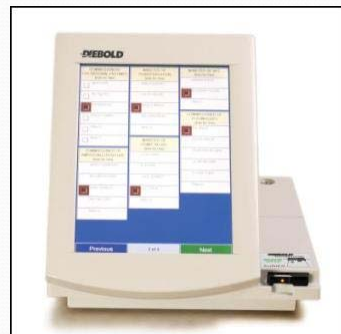
## Enhanced DRE

- Use a DRE *exactly* as before.
- After selections are complete, give voter a (printed) receipt, ask one additional question ...  
*“Do you want to cast this ballot?”*
- If **YES** ... ballot is recorded and confirmation receipt is provided.
- If **NO** ... cancellation receipt is provided and new vote allowed.



## Enhanced DRE (details)

- The initial receipt includes an encrypted ballot.
- All initial receipts are posted and used to compute and validate tally.







## Tradeoffs

- Enhanced DREs provide good accessibility and E2E capabilities *without* requiring printing, collecting, storing, and other management of printed ballots.
- Enhanced OpScan has better survivability and compatibility with current systems.