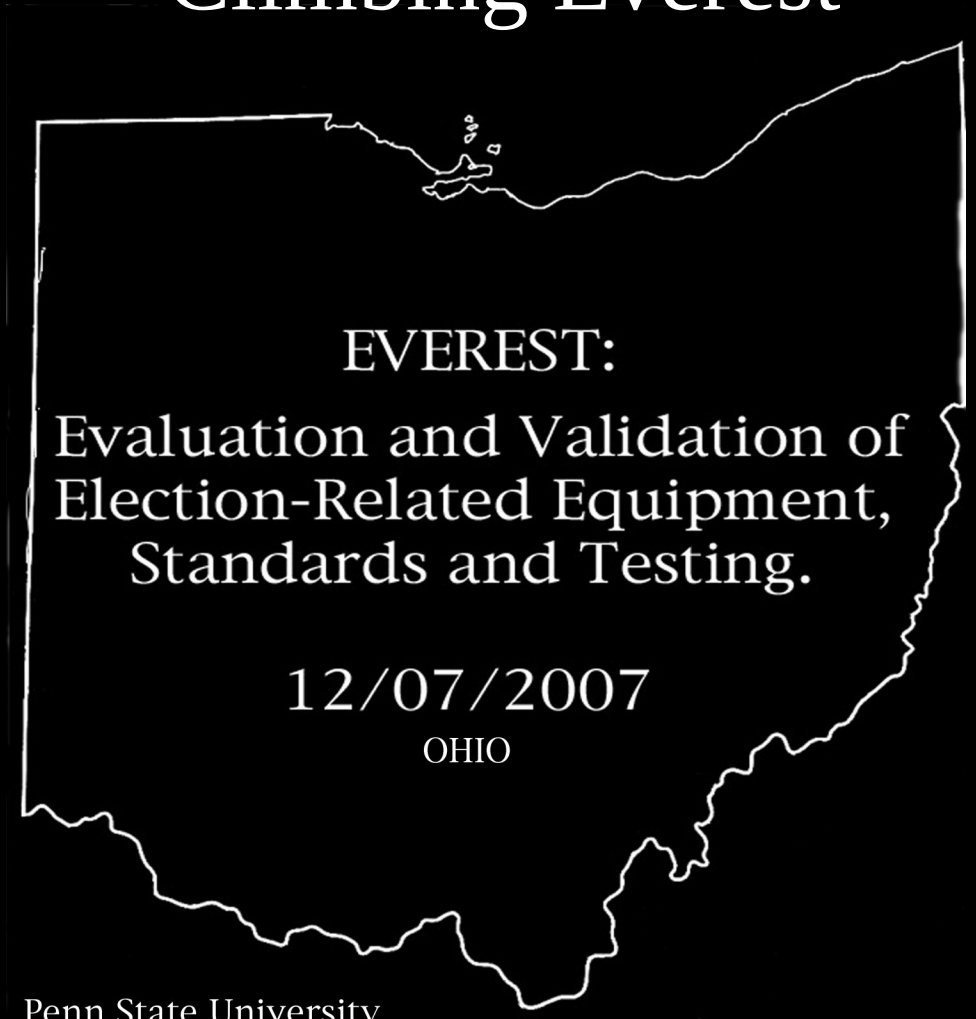
Climbing Everest



Penn State University
University of Pennsylvania
WebWise Security, Inc.

MOUSE

FOR



OVERLORD

Voting 101



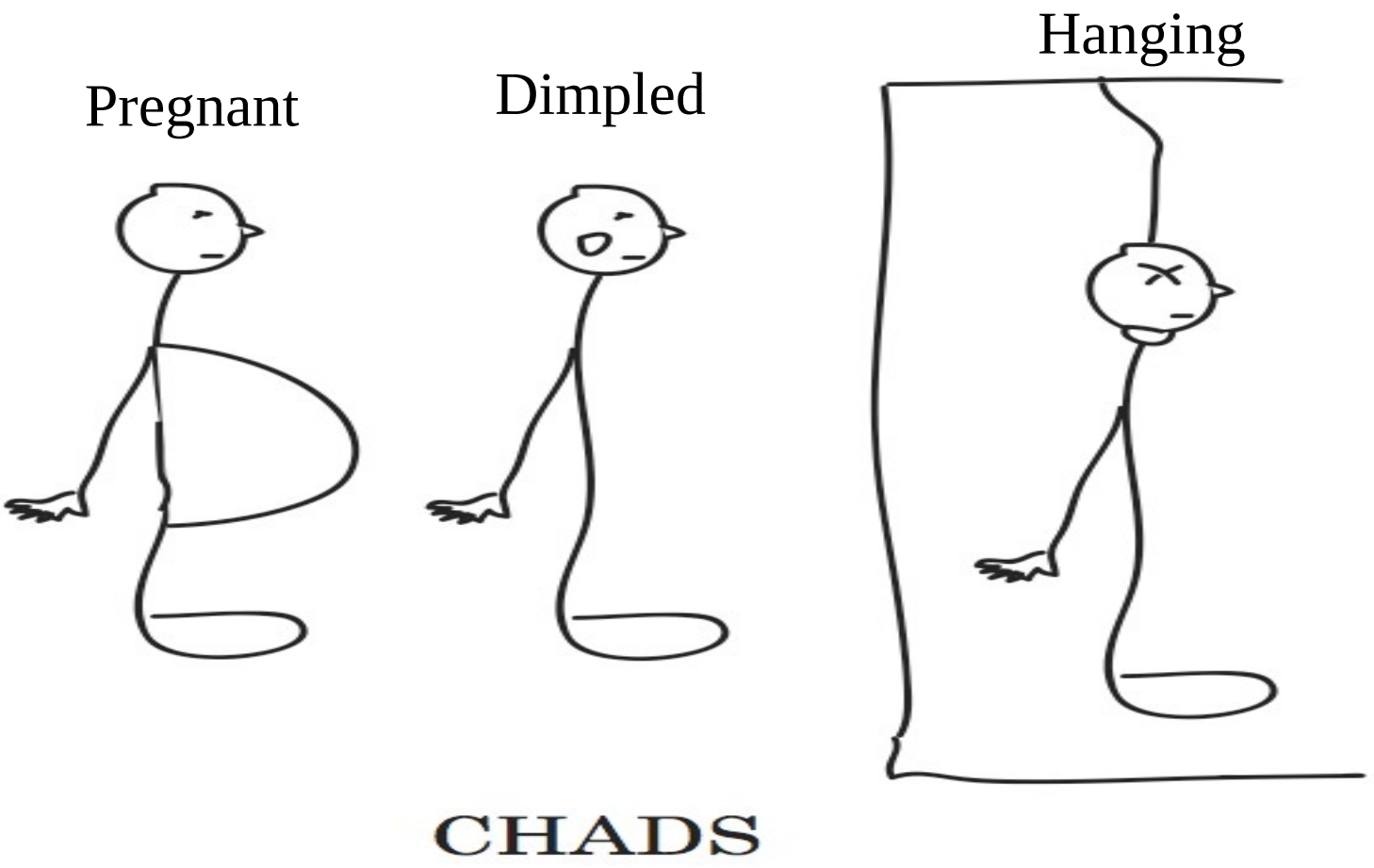
Voting in the US

- Highly decentralized:
  - *Federal* government sets broad standards
  - Each *state* has own laws, rules, requirements
  - Elections run by *counties* (>3000 in US)
  - Voting takes place in neighborhood *precincts*
    - tens, hundreds or thousands per county
- Complex:
  - Typical election has many races
  - Precinct may have several different ballots

Feds vs. States



HAVA



- Favorite HAVA quote:

"For States that **do not** use electronic equipment to assist voters with 'detecting errors', they must:

Establish a voter education program

Provide voter with instructions*

*emphasis added

Project Personnel

Pennsylvania State University Team

Patrick McDaniel, *Principal Investigator & Team Lead*

Kevin Butler
Pennsylvania State University

William Enck
Pennsylvania State University

Harri Hursti
Independent Contractor

Steve McLaughlin
Pennsylvania State University

Patrick Traynor
Pennsylvania State University

University of Pennsylvania Team

Matt Blaze, *Team Lead*

Adam Aviv
University of Pennsylvania

Pavol Černý
University of Pennsylvania

Sandy Clark
University of Pennsylvania

Eric Cronin
University of Pennsylvania

Gaurav Shah
University of Pennsylvania

Micah Sherr
University of Pennsylvania

WebWise Security, Inc.

Giovanni Vigna, *Team Lead*

Richard Kemmerer
WebWise Security, Inc.

Davide Balzarotti
WebWise Security, Inc.

Greg Banks
WebWise Security, Inc.

Marco Cova
WebWise Security, Inc.

Viktoria Felmetsger
WebWise Security, Inc.

William Robertson
WebWise Security, Inc.

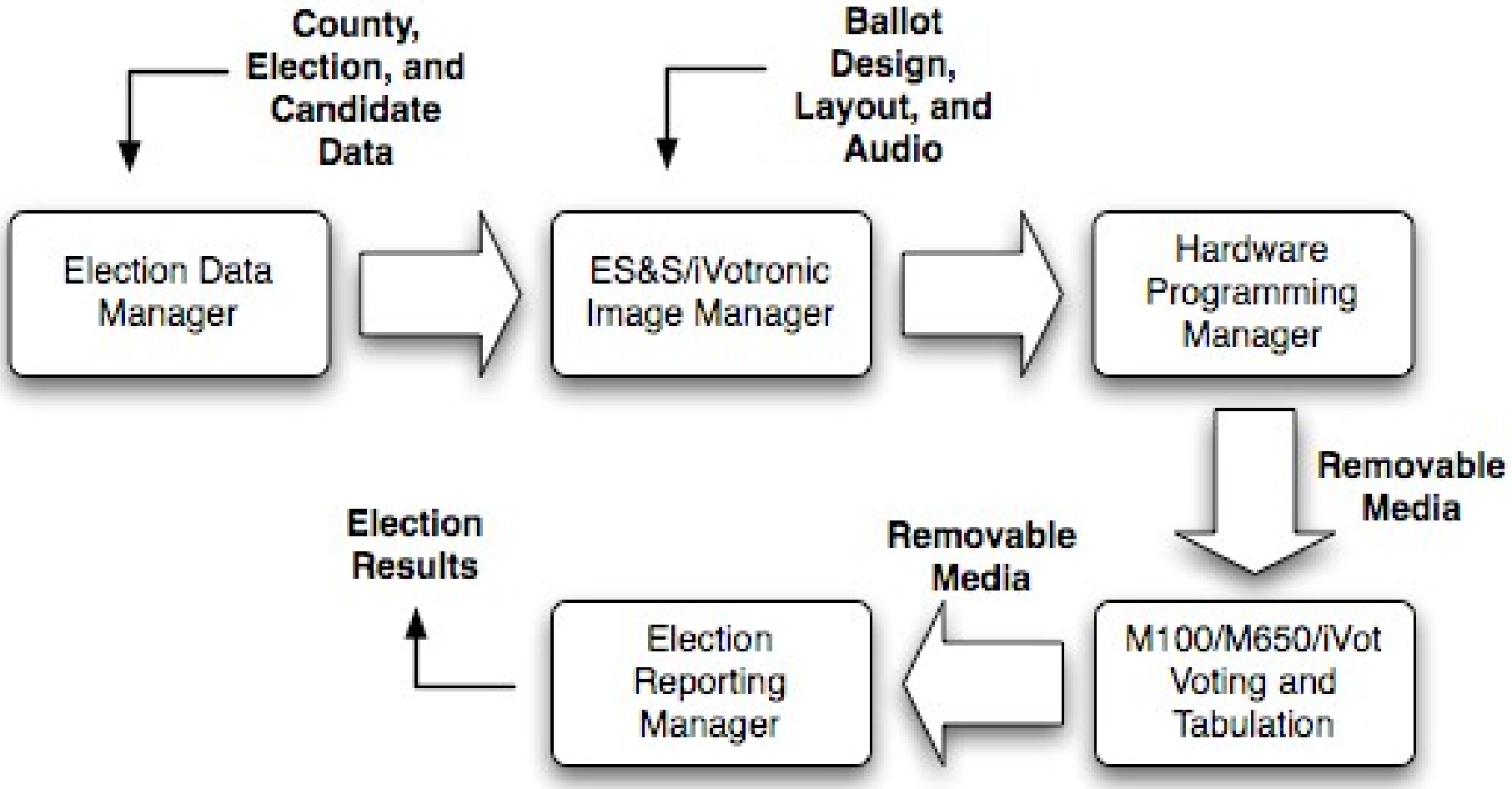
Fredrik Valeur
WebWise Security, Inc.

Policy and Document Consultants

Joseph Lorenzo Hall
University of California, Berkeley

Laura Quilter
University of California, Berkeley

ES&S Structure



Computerized Voting

- Direct Recording Electronic (DRE)
  - specialized voting computer, typically with touch-screen interface
  - records voter selections internally
- Precinct Counted Optical Scan
  - voter fills out a paper ballot (fill in circles)
    - ballot marking devices can assist disabled
  - voter inserts ballot into precinct ballot reader, which either accepts ballot and records vote or rejects and returns ballot to voter
- Centrally (County) Counted Optical Scan
  - absentee ballots



The Horror, the Horror

27.8 Hart VBO Vulnerabilities . . . 307
27.8.1 The VBO record is easily manipulatable by an eSlate program . . . 307
27.8.2 VBO printer allows the paper to be rewound . . . 307
27.8.3 VBO ballots are printed sequentially . . . 307
27.9 Hart Tally Vulnerabilities . . . 307
27.9.1 The Tally interface allows a Tally administrator to "adjust vote totals" . . . 307
27.9.2 Precinct IDs are improperly handled by the system . . . 307
27.9.3 Users can tally unclosed or corrupted MBBs . . . 307
27.9.4 MBBs are only processed if the Tally database allows it . . . 307
27.9.5 Rally and Tally allow a user to accept previously unrecognized certificates . . . 308
27.10 Hart Ballot Now Vulnerabilities . . . 308
27.10.1 Ballot Now ballot counters are stored in a database . . . 308

28 Hart Private Report - New Issues **309**
28.1 Hart General Vulnerabilities . . . 309
28.1.1 An MBB image can be copied and restored without any credentials. . . . 309
28.1.2 EMS systems make improper use of the Windows registry . . . 309
28.1.3 Hart EMS passwords can be bypassed . . . 309
28.1.4 Hart EMS audit logs can be modified or erased . . . 309
28.2 Hart eCM Vulnerabilities . . . 309
28.2.1 eCM keys may be quietly recorded to a debug file . . . 309
28.3 Hart eScan Vulnerabilities . . . 310
28.3.1 The flash memory containing the eScan executable and file system can be replaced . 310
28.3.2 The eScan runs a telnet server . . . 310
28.3.3 The eScan scanner surface can be occluded to affect ballot processing . . . 310
28.3.4 The eScan ballot box collecting votes allows vote order to be reconstructed . . . 310
28.3.5 The eScan ballot box is vulnerable to attacks that may destroy ballots . . . 310
28.3.6 The eScan may be modified to allow casting of duplicate ballots . . . 310
28.3.7 The eScan has an open interface allowing erasure of vote and audit log records . . . 310
28.3.8 The Premier ballot box key works in the Hart ballot box . . . 310
28.3.9 New Vulnerability 09 . . . 311
28.4 Hart JBC Vulnerabilities . . . 311
28.4.1 The JBC can rapidly create an unlimited number of access codes on election day . . . 311
28.4.2 The JBC has an open interface allowing erasure of vote and audit log records . . . 311
28.4.3 JBC/eSlate voting can be completely automated . . . 311
28.5 Hart VBO Vulnerabilities . . . 311
28.5.1 The VBO Printer is controlled via an accessible 1/8" port . . . 311
28.5.2 The serial number of the VBO can be modified . . . 311
28.5.3 The VVPAT paper record may be forged . . . 311
28.6 Hart Tally Vulnerabilities . . . 312

Sorry there are so few,
we were limited on time.

Lines of Code vs. % of Market Share*

ES&S - 670000+ - > 40% market share

Premier- 334000+ - > 40% market share

Other > 20% :

Hart - 300000+

Sequoia - 800000+

*sorry, there's no correlation



My Buffer Overfloweth

If it’s good enough for a minibar…




Hart
Billet Dpt
Key
Hart
Hart
Billet Dpt
Key
Hart




VOTE


291656
291657
291656
291655
291654
291653
291652

Any Port in a Storm




BUY ME!







“With a little token…”

“Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin”

-- John Von Neumann, 1951

“Random numbers should not be generated with a method chosen at random”

-- Donald Knuth, The Art of Computer Programming Vol 2

“The best defense against logic is ignorance”

-- anon

Well… it has passwords and encryption.

It’s not a backdoor, it’s a feature

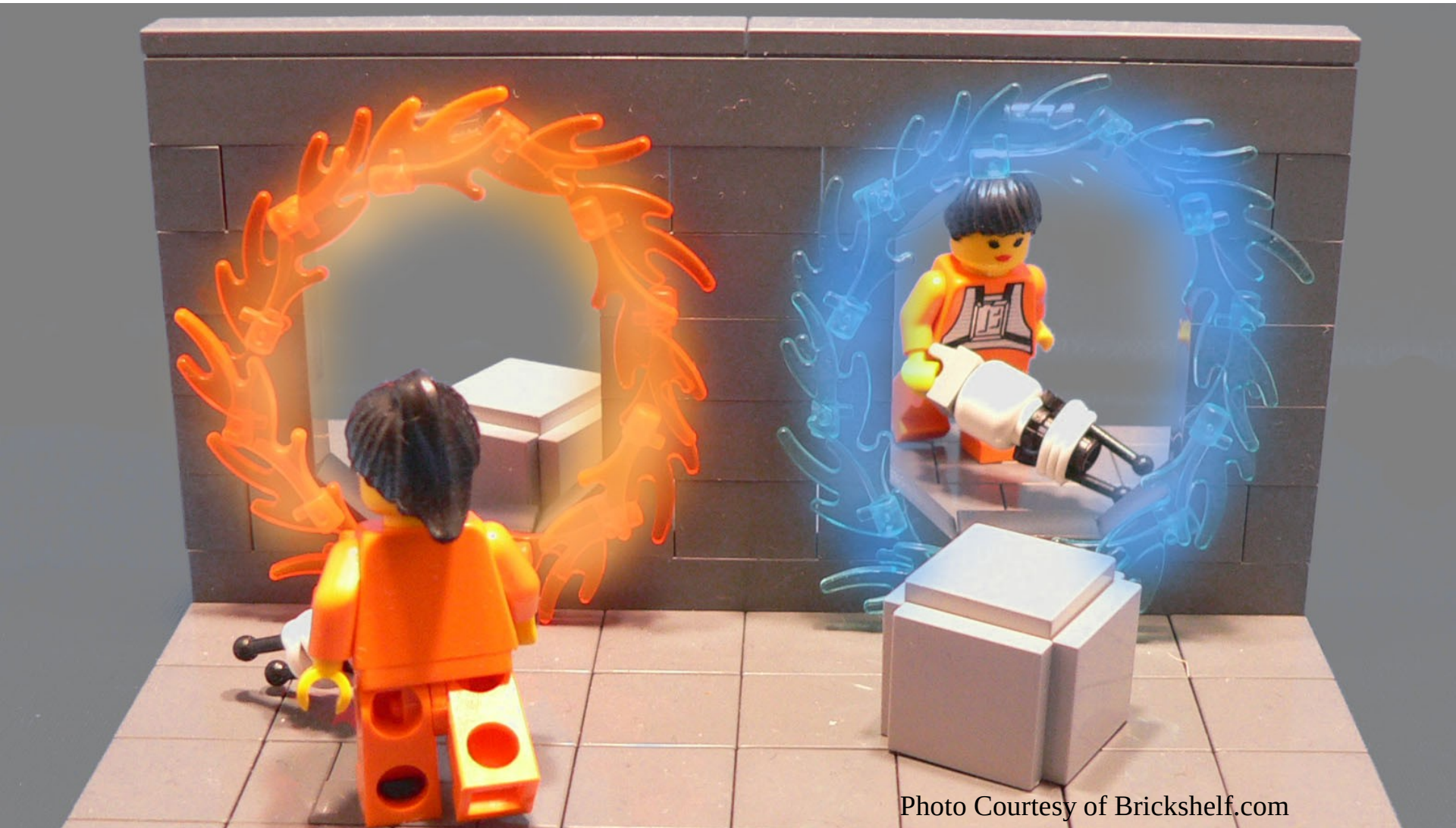


Photo Courtesy of Brickshelf.com



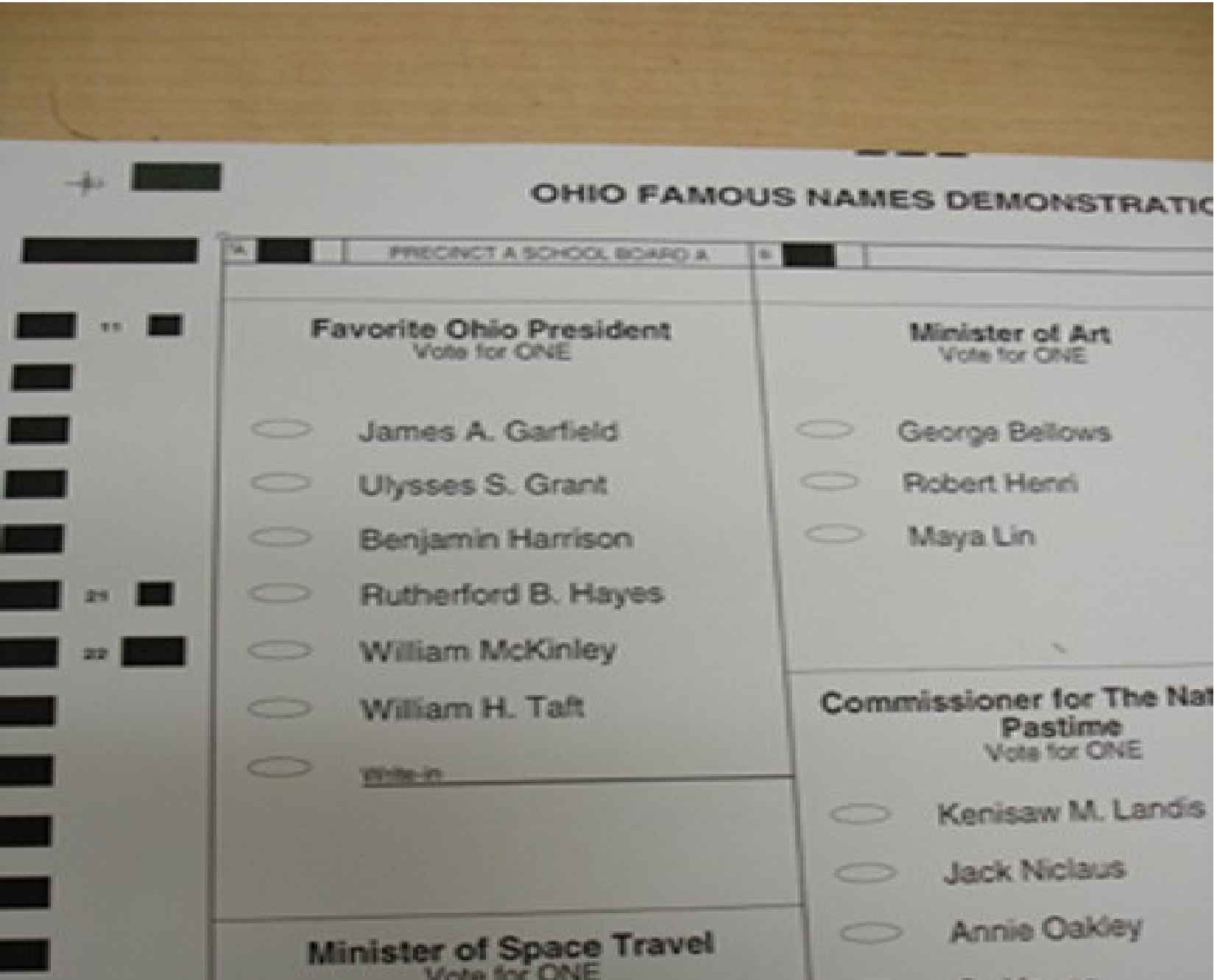
i’m in ur DRE, changin’ ur votes


VOTE
iVotronic Terminal Initialization
Press the VOTE button to start the Initialization Process.
Press the touch screen to EXIT the Initialization Process.
Following the Initialization Process the iVotronic Terminal will contain the following Passwords:
DRE Password: EVEREST
Service Menu Password: EVEREST
Election Central Menu Password: EVEREST
Clear and Test Password: EVEREST
Override Password: EVEREST
Lock Unlock Password: EVEREST
Upload Firmware Password: EVEREST
Qualification Code Password: EVEREST
iVotronic

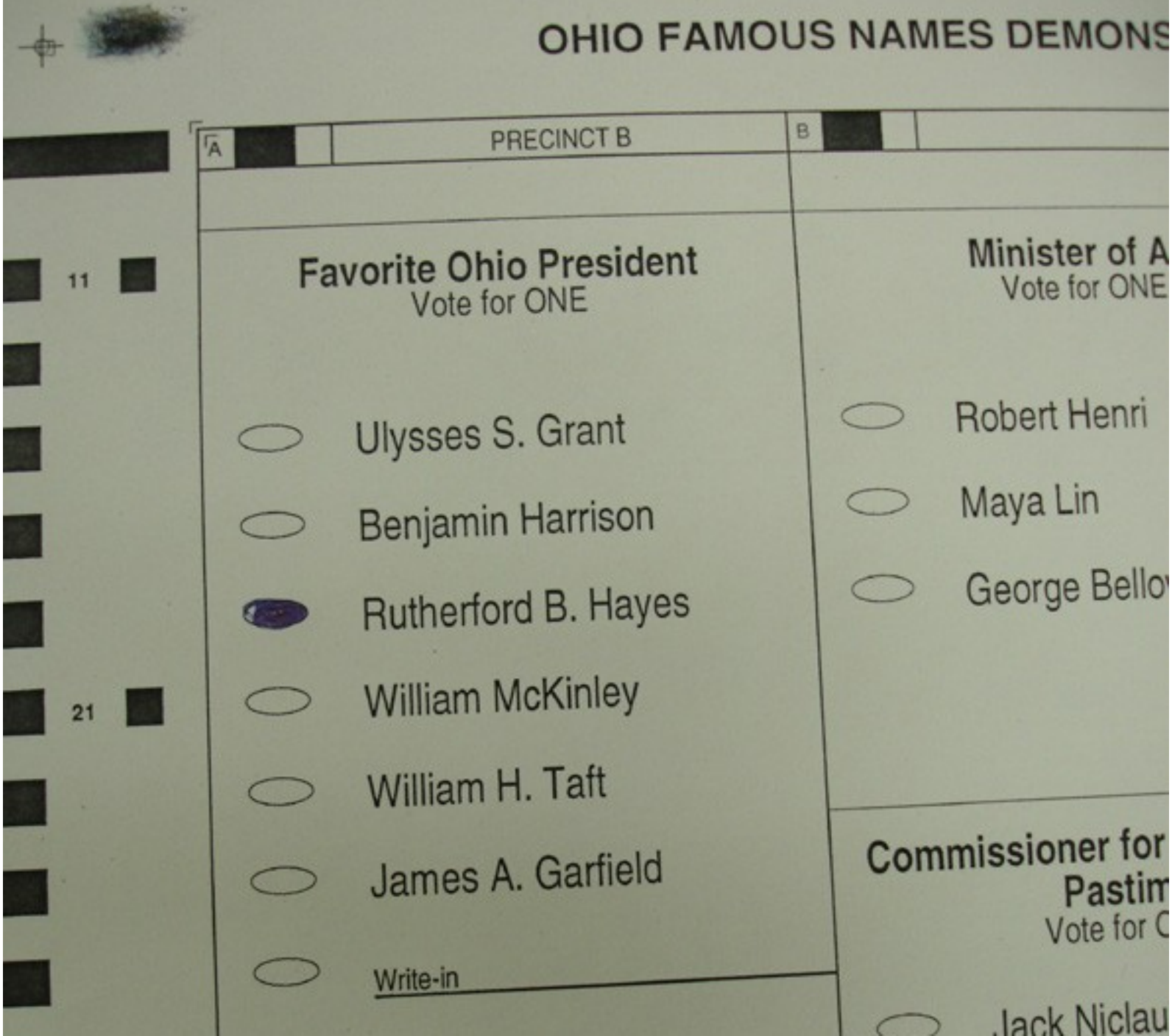

ABSENTEE MODE
EVEREST software installed :)
REPORTS
FORMAT
GRAND TOTALS
PREC. PROCESSED
TOTALS BY PRECINCT
LAST PRECINCT
LAMP TEST
STOP
START


iMedia powered by GNU GRUB version 0.97 (640K lower / 228288K upper memory)
PennState alternative voting-OS Linux
PennState alternative voting-OS Linux Red Team
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
HART
intercivic

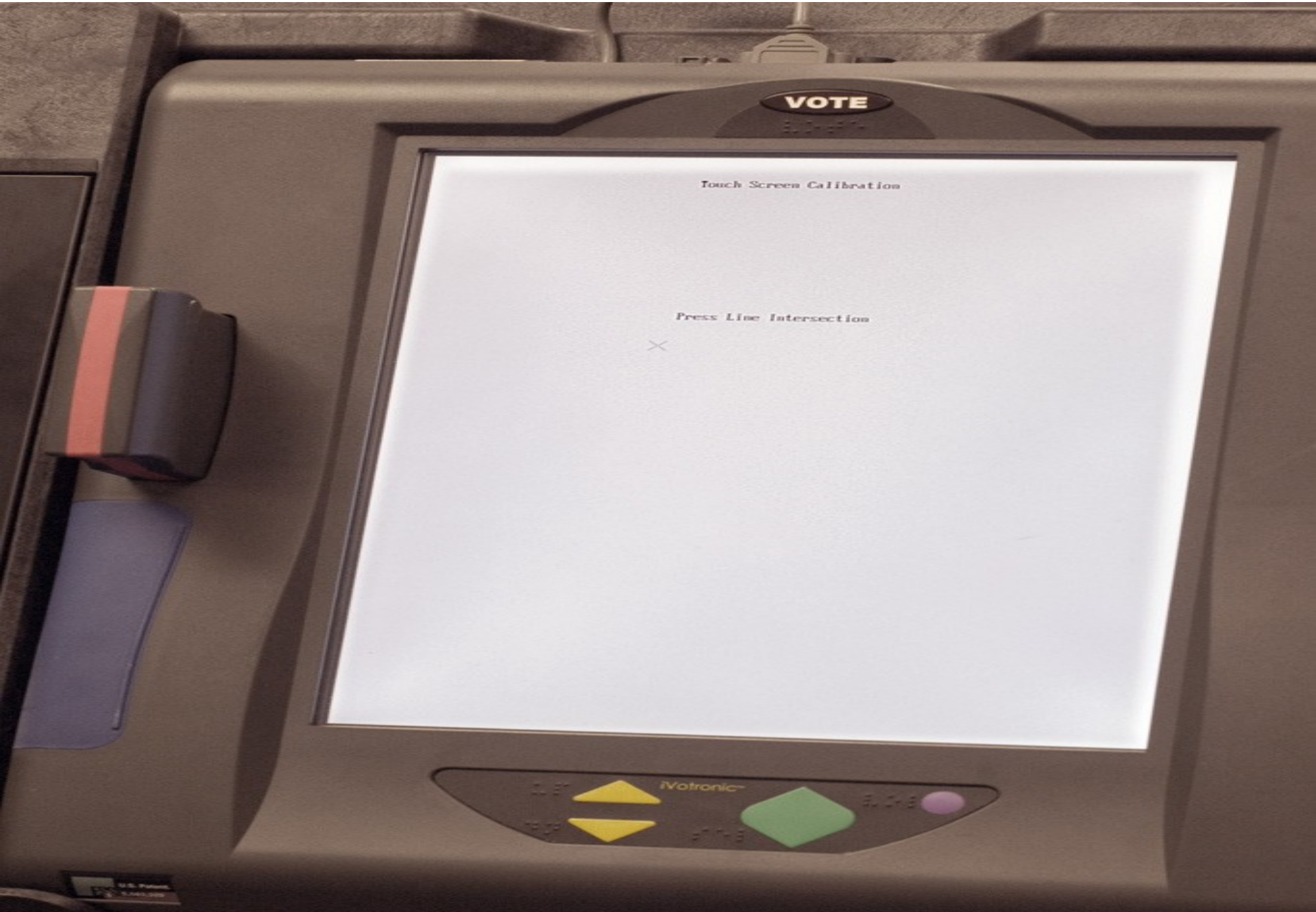
Give me a P


OHIO FAMOUS NAMES DEMONSTRATIO
PRECINCT A SCHOOL BOARD A
Favorite Ohio President
Vote for ONE
James A. Garfield
Ulysses S. Grant
Benjamin Harrison
Rutherford B. Hayes
William McKinley
William H. Taft
Minister of Art
Vote for ONE
George Bellows
Robert Henri
Maya Lin
Commissioner for The Nat
Pastime
Vote for ONE
Kenisaw M. Landis
Jack Niclaus
Annie Oakley
Minister of Space Travel


OHIO FAMOUS NAMES DEMONSTRATION
PRECINCT 8
Favorite Ohio President
Vote for ONE
Ulysses S. Grant
Benjamin Harrison
Rutherford B. Hayes
William McKinley
William H. Taft
James A. Garfield
Write-in
Minister of Art
Vote for ONE
Robert Henri
Maya Lin
George Bellows
Commissioner for The Natio
Pastime
Vote for ONE
Jack Niclaus
Annie Oakley
Cy Young
Kenisaw M. Landis
Minister of Space Travel
Vote for ONE
Nancy Currie
John Glenn
Judith Resnick
Neil Armstrong
Minister of Musi
Vote for ONE


OHIO FAMOUS NAMES DEMONS
PRECINCT B
A
B
11
21
Favorite Ohio President
Vote for ONE
Ulysses S. Grant
Benjamin Harrison
Rutherford B. Hayes
William McKinley
William H. Taft
James A. Garfield
Write-in
Minister of A
Vote for ONE
Robert Henri
Maya Lin
George Bello
Commissioner for
Pastim
Vote for
Jack Niclau

Give me an R


VOTE
Touch Screen Calibration
Press Line Intersection
iVotronic

Give me a U


VOTER CARD ENCODER
DIEBOLD
Unlimited
Votes
ON
OFF
1
2
3
NO
4
5
6
7
8
9
*
0
#
YES

- Give me a C -

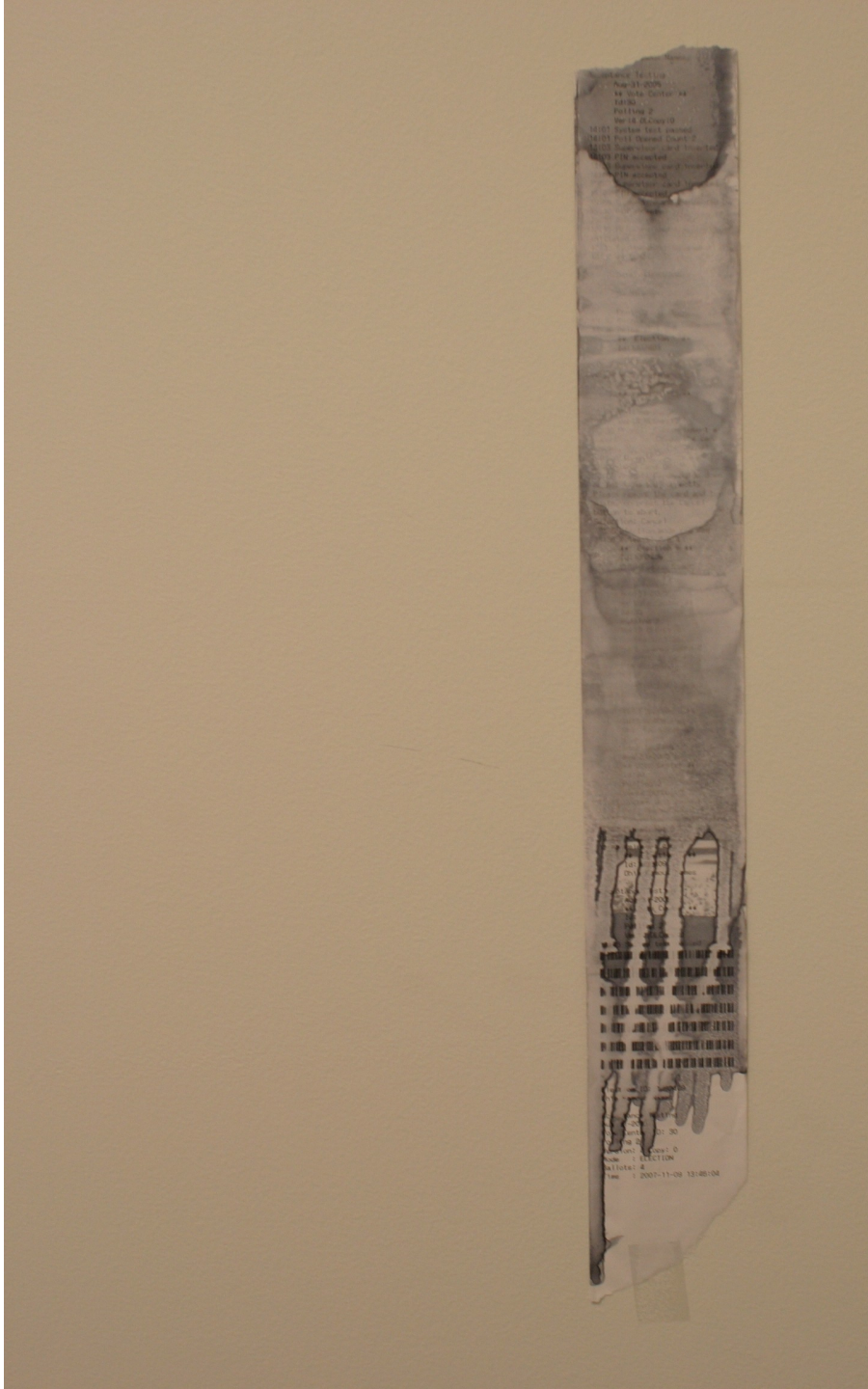
Cast multiple votes,

Erase audit logs

Disable VVPAT

Zero Totals

IOW, *Anything*



What's that Spell?

PRUC!

of course it may spell PRUC, but it means…

VIRAL PROPAGATION

Conclusions

- All academic, right?

Conclusions

- All academic, right?
- Unsafe at any speed.

Conclusions

- All academic, right?
- Unsafe at any speed
- What can you do?

Conclusions

- All academic, right?
- Unsafe at any speed
- What can you do?
  - VOTE!

Conclusions

- All academic, right?
- Unsafe at any speed
- What can you do?
  - VOTE!
  - Become a Poll Worker

Conclusions

- All academic, right?
- Unsafe at any speed
- What can you do?
  - VOTE!
  - Become a Poll Worker
  - Build a better system

MOUSE

FOR



OVERLORD

Shmoocon 2008



CATS: ALL YOUR VOTE ARE BELONG TO US.