End-to-End Verifiable Election Technologies

Josh Benaloh

Senior Cryptographer
Microsoft Research

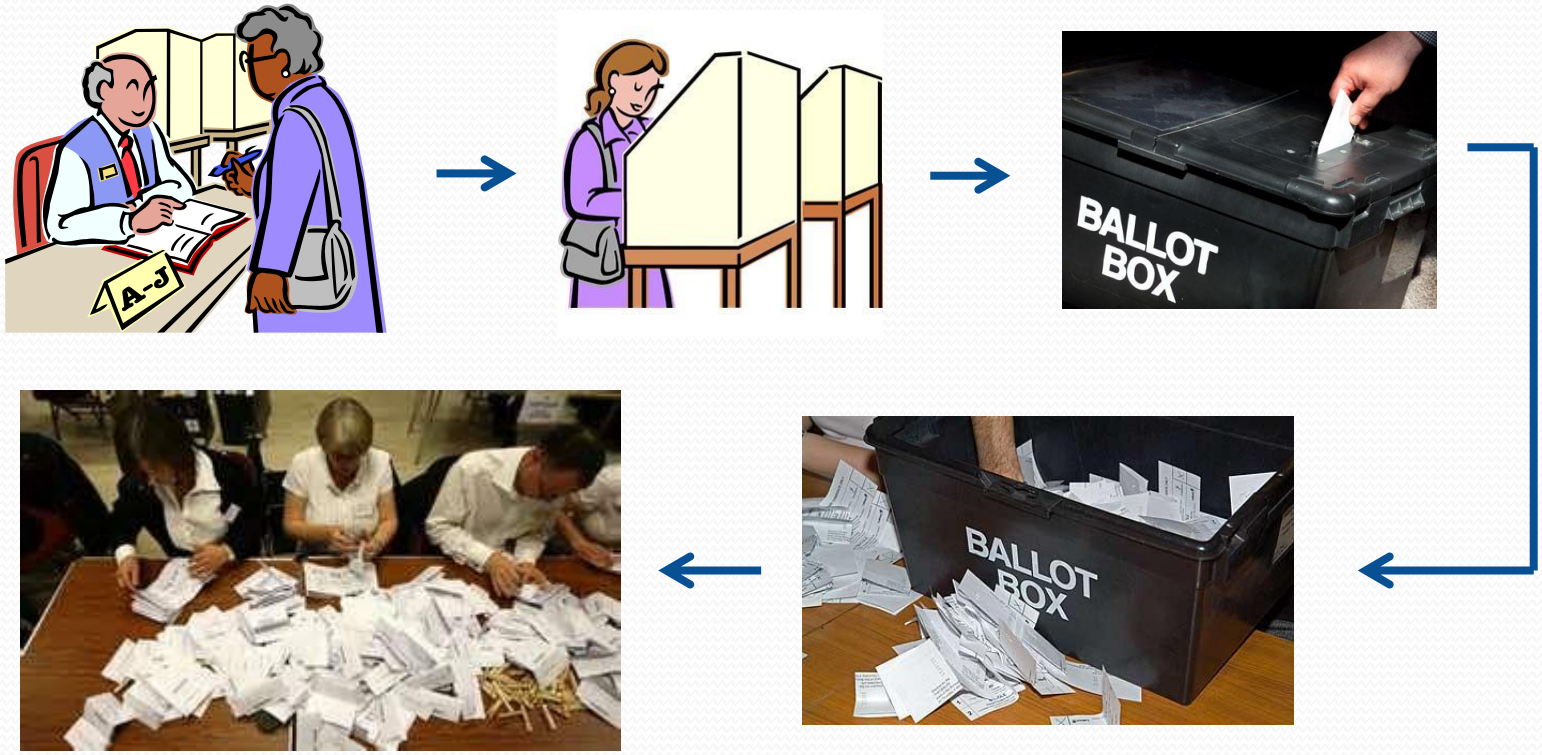
What E2E-Verifiability is *not* …

New

E2E-Verifiability dates back more than 30 years.

What E2E-Verifiability is *not* …

So-called "Voter-Verifiability"



What it's *not*

End-to-End Verifiability is *not* …

- A kind of Internet voting system
- A kind of remote voting system
- A kind of electronic voting system
- A kind of voting system

E2E is a property

End-to-end verifiability is a property of an *election.*

- Voters can check that their selections have been accurately recorded.
- Anyone can check that all recorded votes have been accurately counted.

An E2E-Verifiable Election

Voter Name	Vote
Alice Smith	Jefferson
Bob Williams	Adams
Carol James	Adams
David Fuentes	Jefferson
Ellen Chu	Jefferson

Totals	
Jefferson	3
Adams	2

An E2E-Verifiable Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

Totals	
Jefferson	3
Adams	2

An E2E-Verifiable Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

Totals	
Jefferson	3
Adams	2

An E2E-Verifiable Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

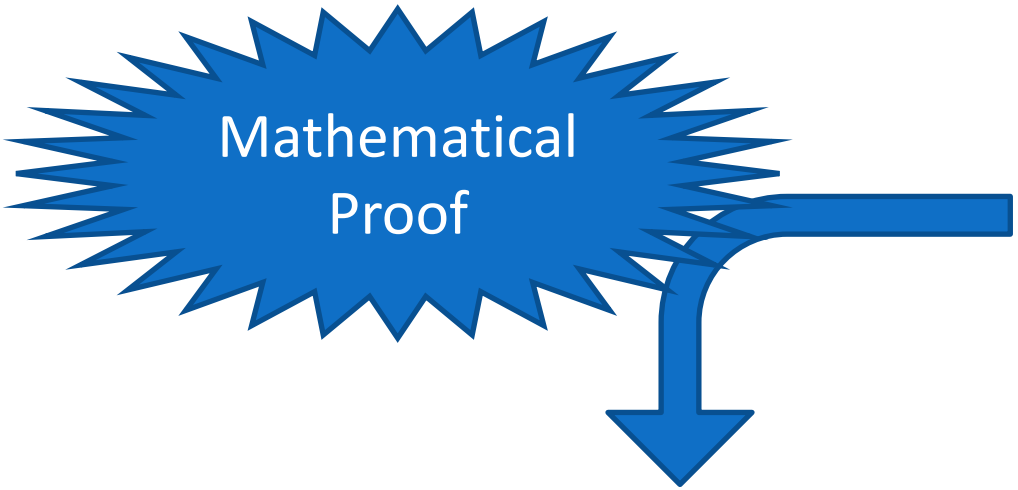
Totals	
Jefferson	3
Adams	2

An E2E-Verifiable Election

X37BM6YPM
2J8CNF2KQ
VRSF5JQWZ
MW5B2VA7Y
8VPPS2L39

Totals	
Jefferson	3
Adams	2

An E2E-Verifiable Election



X37BM6YPM
2J8CNF2KQ
VRSF5JQWZ
MW5B2VA7Y
8VPPS2L39

Totals	
Jefferson	3
Adams	2

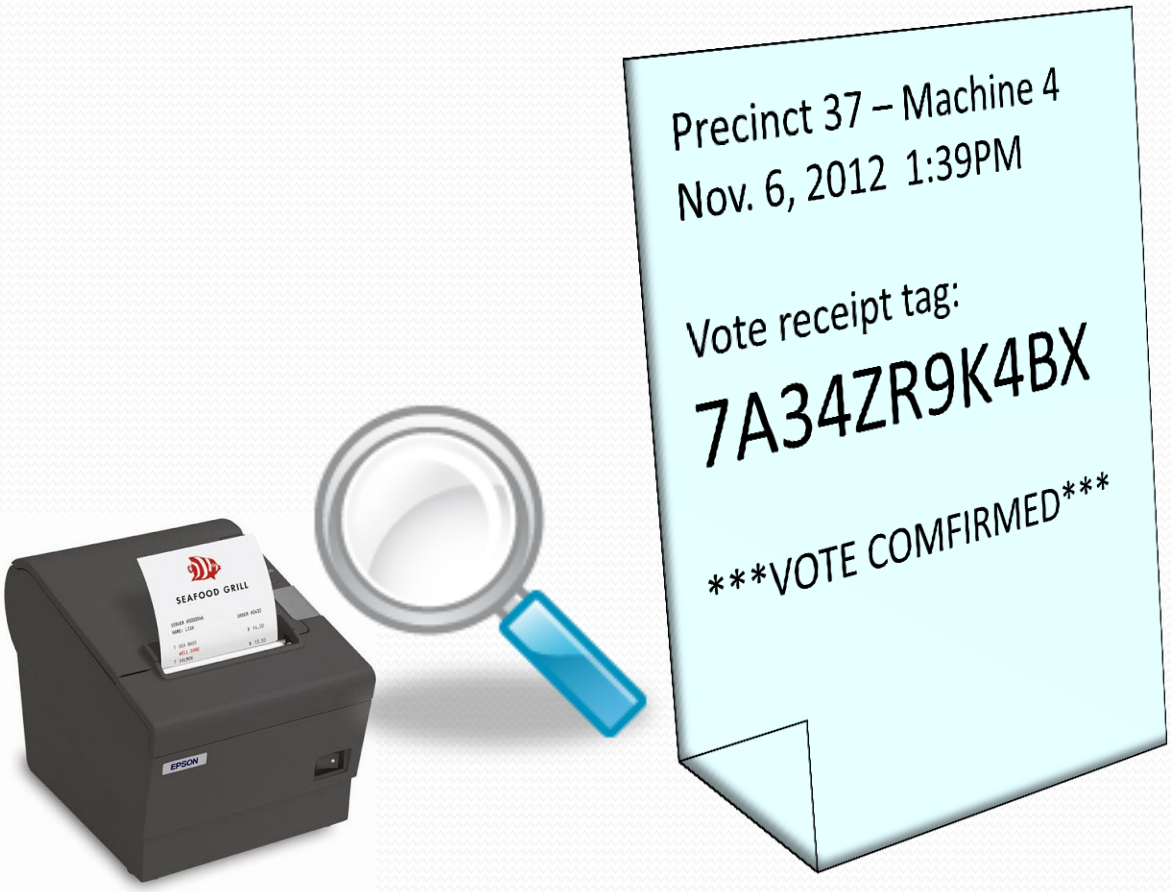
The Voter's Perspective

Systems that produce verifiable elections can be built to look exactly like current systems …

- paper-based
- fully-electronic
- in-person
- remote

… with one addition …

A Verifiable Receipt



The Voter's Perspective

Voters can …

- Use receipts to check their results are properly recorded on a public web site.
- Throw their receipts in the trash.

- Write and use their own election verifiers
- Download applications from sources of their choice to verify the mathematical proof of the tally.
- Believe verifications done by their political parties, LWV, ACLU, etc.
- Accept the results without question.

Some systems producing verifiable elections …

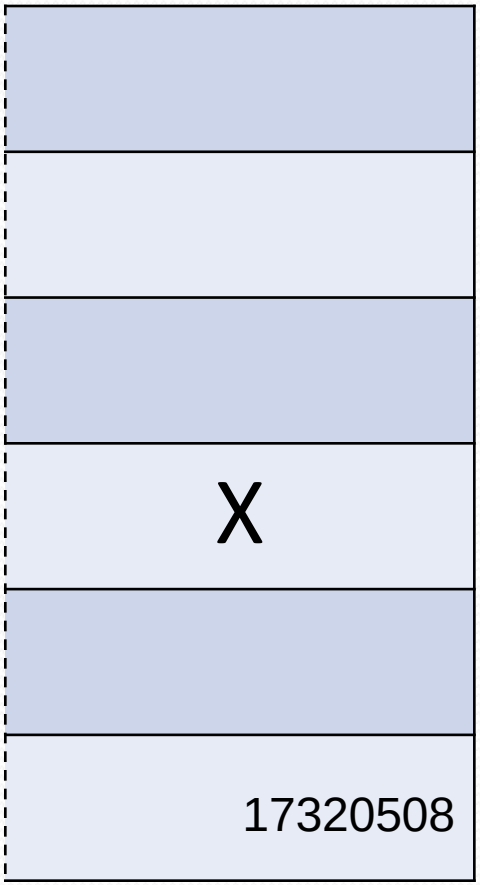
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	
David	
	17320508

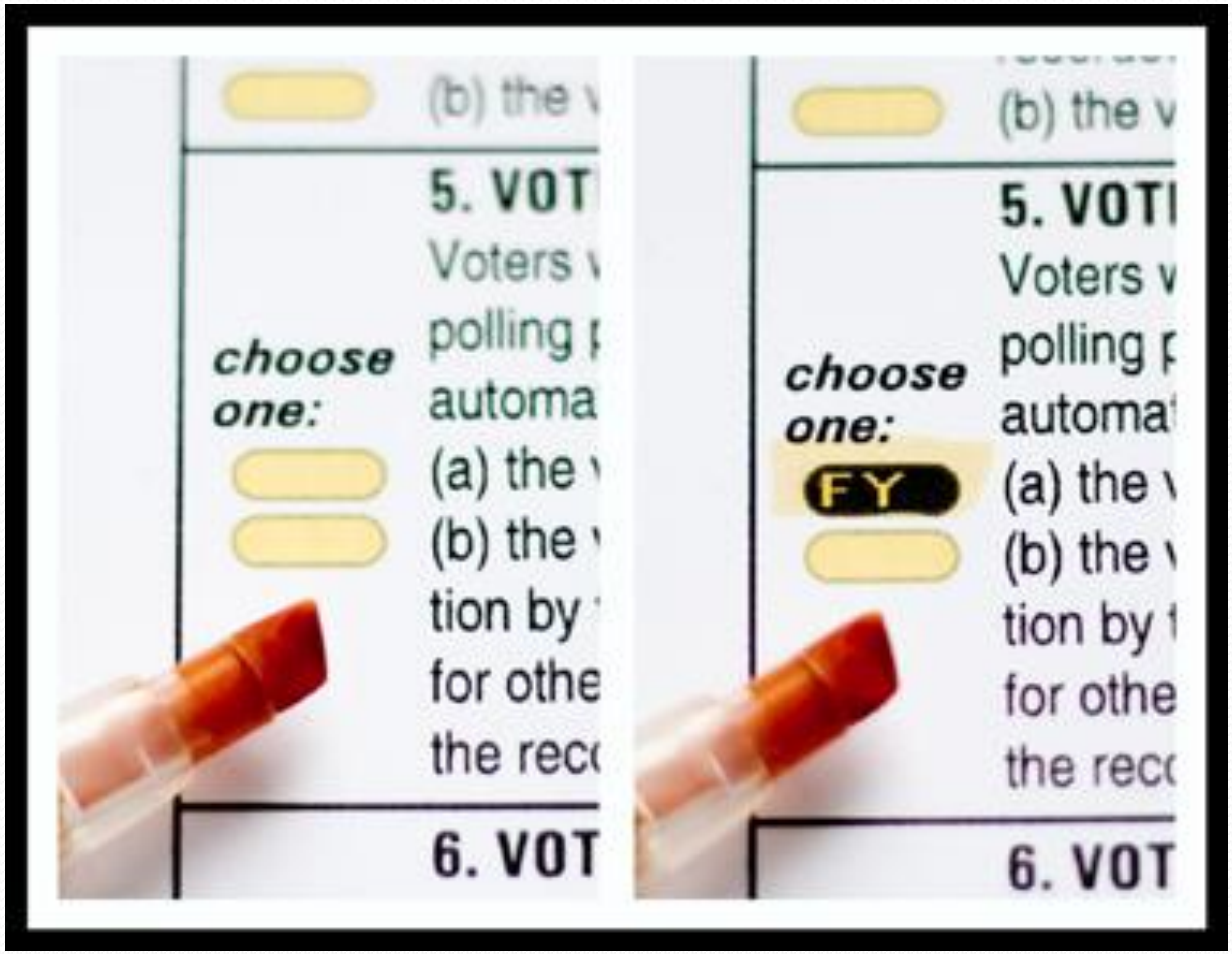
Prêt à Voter Ballot

Bob	
Eve	
Carol	
Alice	X
David	
	17320508

Prêt à Voter Ballot



Scantegrity



VeriScan

OFFICIAL BALLOT

CONSOLIDATED GENERAL ELECTION

SANTA BARBARA COUNTY, CALIFORNIA

NOVEMBER 5, 2002

INSTRUCTIONS TO VOTERS: To vote for the candidate of your choice, completely fill in the OVAL to the LEFT of the candidate's name. To vote for a person whose name is not on the ballot, darken the OVAL next to and write in the candidate's name on the Write-in line. To vote for a measure, darken the OVAL next to the word "Yes" or the word "No". All distinguishing marks or erasures are forbidden and make the ballot void. If you tear, deface, or wrongly mark this ballot, return it and get another. VOTE LIKE THIS: ● **VOTE BOTH SIDES**

STATE

GOVERNOR
Vote for One

- ◯ GARY DAVID COPELAND — Chief Executive Officer — Libertarian
- ◯ BILL SIMON — Businessman/Charity Director — Republican
- ◯ REINHOLD GULKE — Electrical Contractor/Farmer — American Independent
- ◯ GRAY DAVIS — Governor of the State of California — Democratic
- ◯ IRIS ADAM — Business Analyst — Natural Law
- ◯ PETER MIGUEL CAMEJO — Financial Investment Advisor — Green
- ◯ Write-In

LIEUTENANT GOVERNOR
Vote for One

- ◯ PAT WRIGHT — Ferret Legalization Coordinator — Libertarian
- ◯ PAUL JERRY HANNOSH — Educator/Businessman — Reform
- ◯ BRUCE MC PHERSON — California State Senator — Republican
- ◯ KALEE PRZYBYLAK — Public Relations Director — Natural Law
- ◯ CRUZ M. BUSTAMANTE — Lieutenant Governor — Democratic
- ◯ JIM KING — Real Estate Broker — American Independent
- ◯ DONNA J. WARREN — Certified Financial Manager — Green
- ◯ Write-In

INSURANCE COMMISSIONER
Vote for One

- ◯ DALE F. OGDEN — Insurance Consultant/Actuary — Libertarian
- ◯ DAVID I. SHEIDLOWER — Financial Services Executive — Green
- ◯ GARY MENDOZA — Businessman — Republican
- ◯ JOHN GARAMENDI — Rancher — Democratic
- ◯ STEVE KLEIN — Businessman — American Independent
- ◯ RAUL CALDERON, JR. — Health Researcher/Educator — Natural Law
- ◯ Write-In

MEMBER, STATE BOARD OF EQUALIZATION
2ND District
Vote for One

- ◯ TOM Y. SANTOS — Tax Consultant/Realtor — Democratic
- ◯ BILL LEONARD — State Lawmaker/Businessman — Republican
- ◯ Write-In

UNITED STATES REPRESENTATIVE

24TH District
Vote for One

- ◯ ELTON GALLEGLY — U.S. Representative — Republican

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE JUDITH M. ASHMANN be elected to the office for the term prescribed by law?

◯ YES ◯ NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE KATHRYN DOI TODD be elected to the office for the term prescribed by law?

◯ YES ◯ NO

FOR PRESIDING JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION THREE

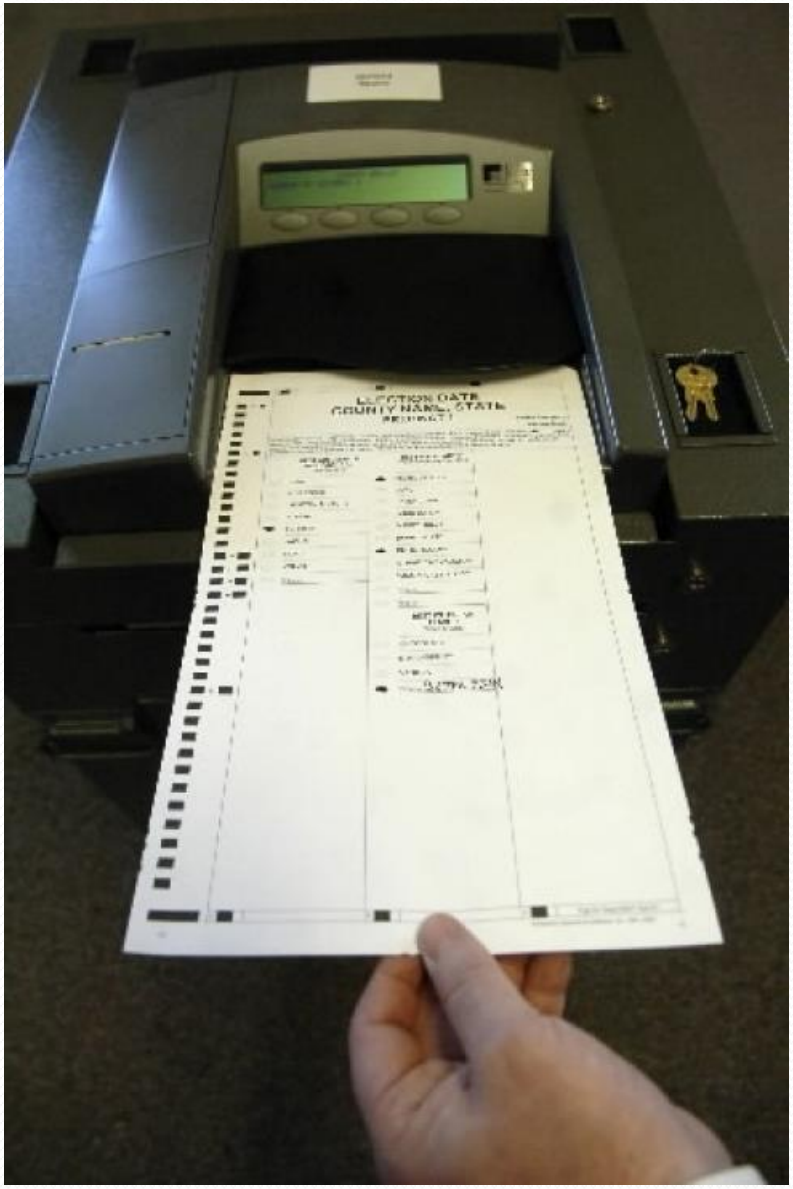
Shall PRESIDING JUSTICE JOAN DEMPSEY KLEIN be elected to the office for the term prescribed by law?

◯ YES ◯ NO

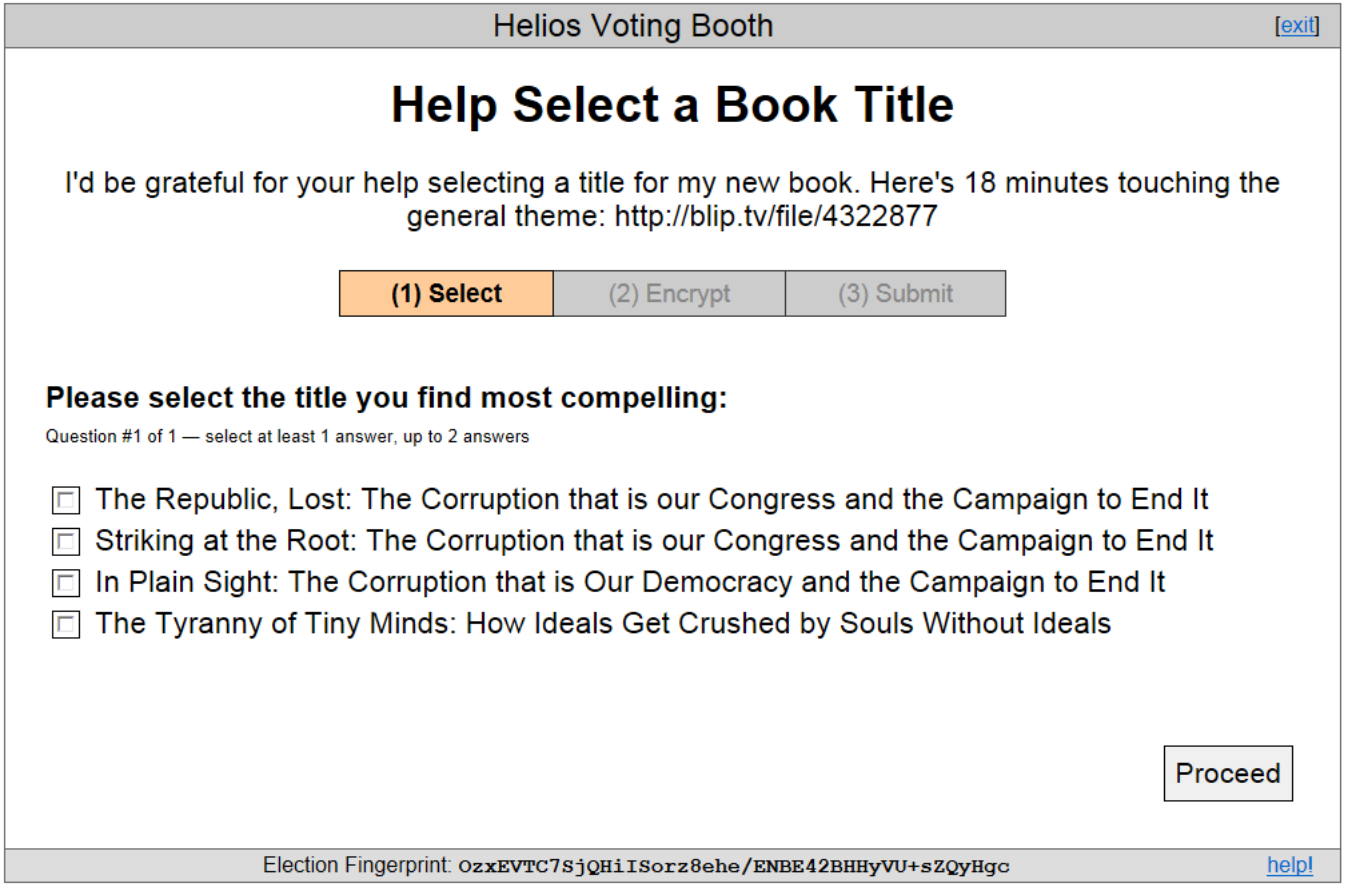
FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION FOUR

Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law?

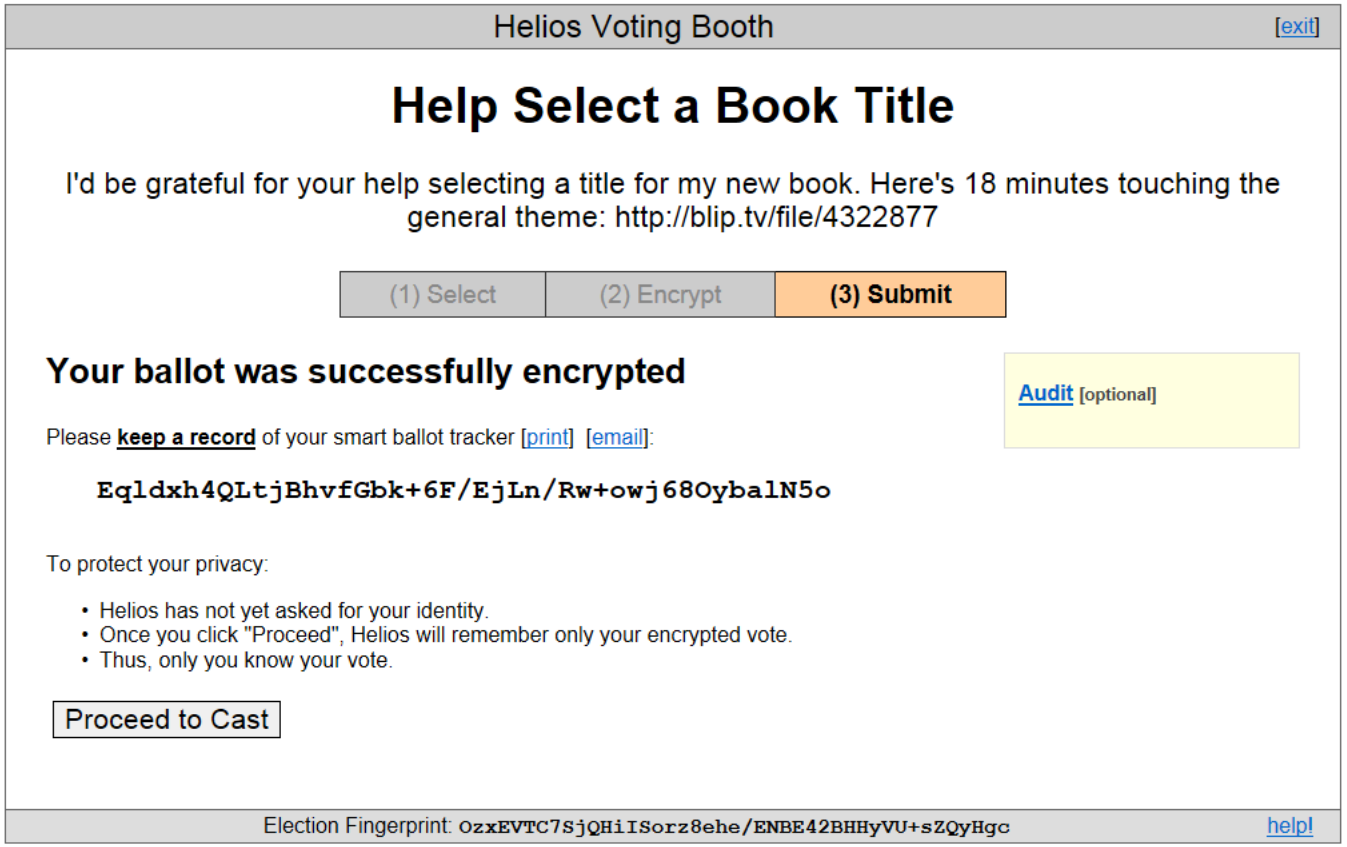
◯ YES ◯ NO



Helios


Helios Voting Booth
[exit]
Help Select a Book Title
I'd be grateful for your help selecting a title for my new book. Here's 18 minutes touching the general theme: http://blip.tv/file/4322877
(1) Select
(2) Encrypt
(3) Submit
Please select the title you find most compelling:
Question #1 of 1 — select at least 1 answer, up to 2 answers
The Republic, Lost: The Corruption that is our Congress and the Campaign to End It
Striking at the Root: The Corruption that is our Congress and the Campaign to End It
In Plain Sight: The Corruption that is Our Democracy and the Campaign to End It
The Tyranny of Tiny Minds: How Ideals Get Crushed by Souls Without Ideals
Proceed
Election Fingerprint: OzxEVTC7SjQHiISorz8ehe/ENBE42BHHyVU+sZQyHgc
help!

Helios


Helios Voting Booth
[exit]
Help Select a Book Title
I'd be grateful for your help selecting a title for my new book. Here's 18 minutes touching the general theme: http://blip.tv/file/4322877
(1) Select
(2) Encrypt
(3) Submit
Your ballot was successfully encrypted
Audit [optional]
Please keep a record of your smart ballot tracker [print] [email]:
Eqldxh4QLtjBhvfGbk+6F/EjLn/Rw+owj68OybalN5o
To protect your privacy:
• Helios has not yet asked for your identity.
• Once you click "Proceed", Helios will remember only your encrypted vote.
• Thus, only you know your vote.
Proceed to Cast
Election Fingerprint: OzxEVTC7SjQHiISorz8ehe/ENBE42BHHyVU+sZQyHgc
help!

STAR-Vote

- Voters use electronic ballot marking devices to indicate their preferences.
- When a voter's selections are completed, the device provides the voter with a paper ballot summary and an encrypted receipt. It also records the encrypted ballot.
- The voter can review the paper ballot summary, and optionally deposit it in a ballot box.
- All encrypted ballots are posted, but the only votes counted are those for which a corresponding paper ballot has been deposited. The remaining ballots are decrypted.

Benefits of E2E-Verifiability

- Strong public assurance of election integrity
- Elimination of trust requirements
- Certification relief

What's Next?

- Research on new designs
- Usability/effectiveness testing
- Regulatory/cultural changes
- Deployment