Voting Systems: From Art to Science

Voting Technology Conference 2001
Pasadena, Calif., March 30-31
Caltech/MIT

Ed Gerck, Ph.D.
egerck@safevote.com
CEO & VP of Technology

2007 Note

This presentation deals with a general model for voting, using Shannon's Communication Theory. The Fundamental Problem of Voting is that the voter must not be able to see that her vote was tallied (to preserve election integrity), and yet the voter must be able to have confidence that the vote was tallied as cast.

The discussion remains timely and valid. The latest experiments in e-voting, and problems with DREs, have confirmed the predictions made in this presentation.

Please also see the presentation at
http://www.vote.caltech.edu/wote01/pdfs/gerck-witness.pdf
for implementation examples of this discussion.

Program

We need to focus on requirements and models first, not on technology!

We need to develop a voting model that can:

1. Explain current systems (analysis tool)
2. Predict the behavior of new systems

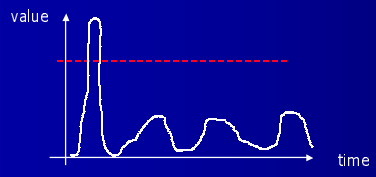
With such a model we should be able to:

1. Improve current systems
2. Develop better systems

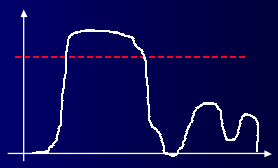
The first requirement is voter privacy!

Accuracy vs Reliability

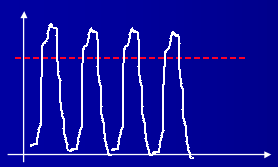
Accuracy affects the spread of one event.
Reliability affects events over time and space.



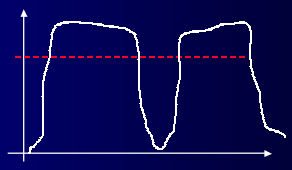
high accuracy, high reliability



low accuracy, high reliability



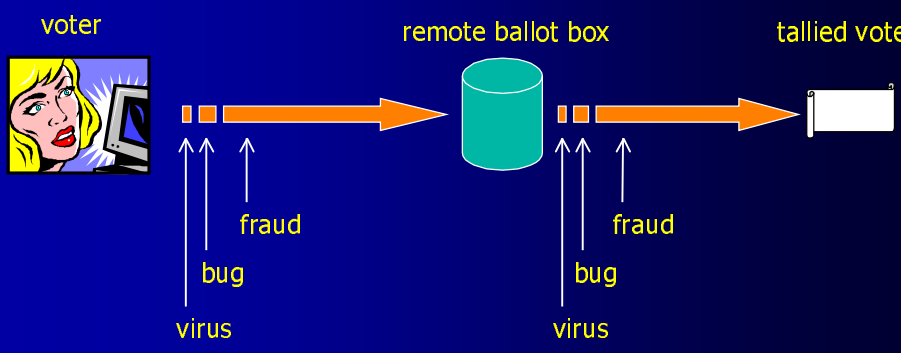
high accuracy, low reliability



low accuracy, low reliability

- Reliability may be close to 100%, but not equal to 100%.
- Accuracy can be 100% in digital systems.

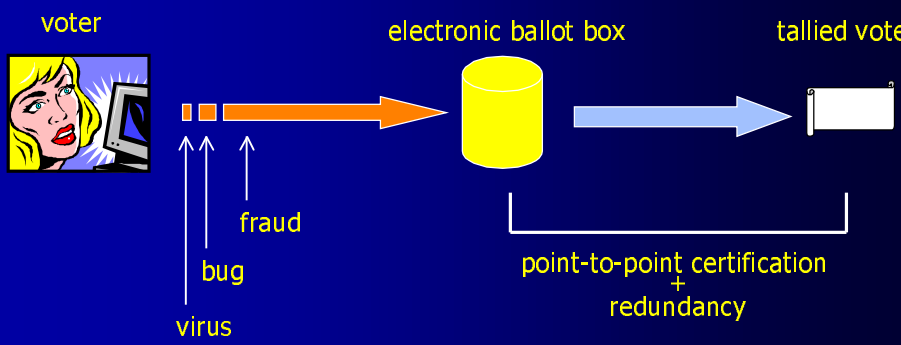
The Fundamental Problem of Network Voting



Low Reliability

The voter cannot see her tallied vote, hence the voter cannot know whether her vote will be counted as selected.

The Fundamental Problem of Electronic Voting

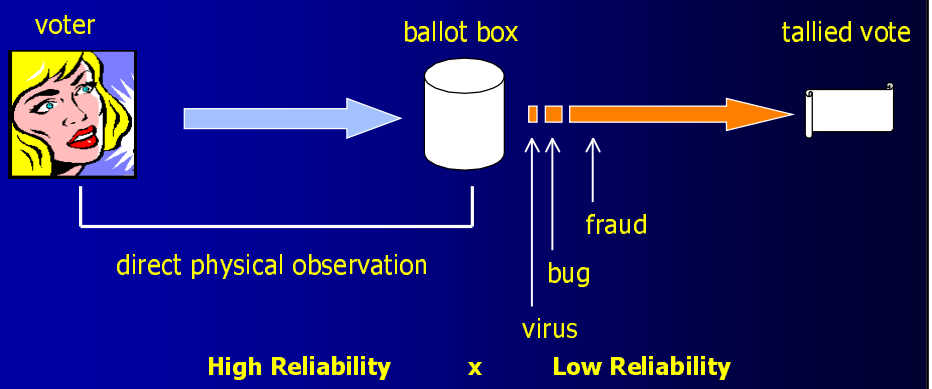


Low Reliability **x** **High Reliability**

Low Reliability

The voter cannot see her tallied vote, hence the voter cannot know whether her vote will be counted as selected.

The Fundamental Problem of Paper Voting

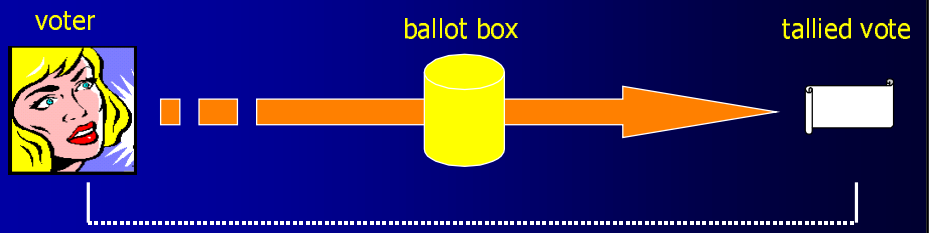


High Reliability **x** **Low Reliability**

Low Reliability

The voter cannot see her tallied vote, hence the voter cannot know whether her vote will be counted as selected.

The Fundamental Problem of Voting



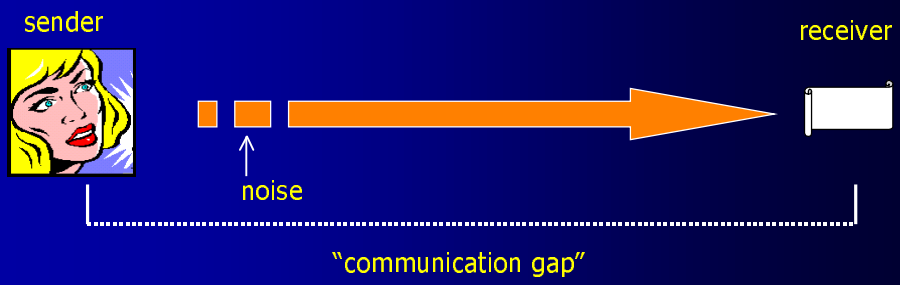
"vote gap"

Low Reliability

The voter cannot see her tallied vote, hence the voter cannot know whether her vote will be counted as selected.

Voting results cannot ever have 100% reliability for more than one voter, even if every voter publicly discloses what her/his vote was, even if we just use paper and pen in all processes and perfectly keep all records. The impossibility of objectively reaching 100% reliability is due to the absolute requirement that no one should be able to prove how a voter voted, not even the voter herself. And yet, society must be confident that the result is reliable.

The Fundamental Problem of Communication

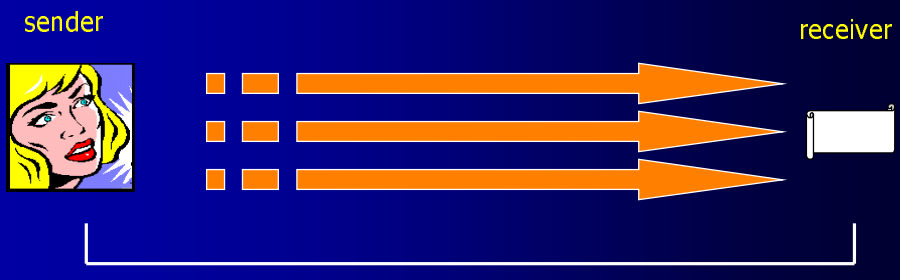


Low Reliability

Shannon (1948): The fundamental problem of communication is that of reproducing at one point a message selected at another point.

The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown.

Solution: Enough Redundancy



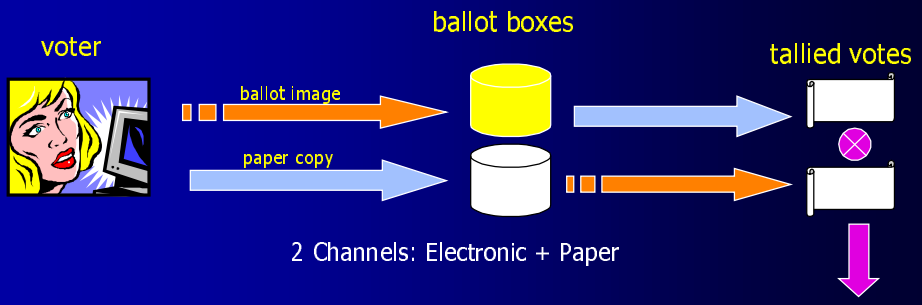
High Reliability

Shannon, 10th Theorem (1948):

Independent channels can be used to send correction data so that all but an arbitrarily small fraction of errors can be corrected. Redundancy ➔ high reliability.

We can only approach the limit of 100% reliability in voting results. The good news is that it is possible to get as close as we desire to 100%. The bad news is that Shannon's theory does not tell us exactly how to do it – we must discover it!

Precinct Voting
Analysis: Electronic Voting + Paper Ballots



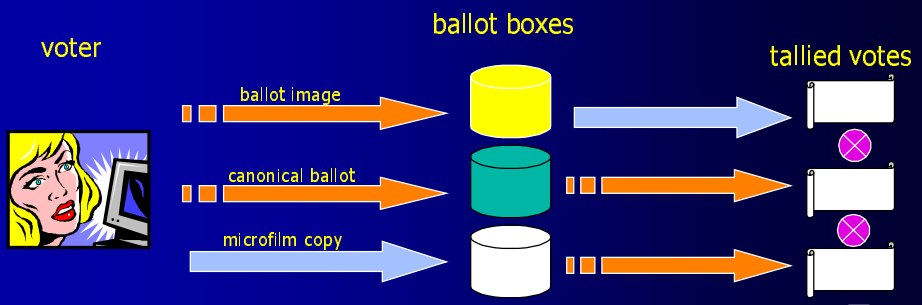
2 Channels: Electronic + Paper

If both channels disagree, the system is indeterminate. ?

Possible solution: accept a difference if it makes no difference.

The solution thus comes by policy, outside the system and defined a priori.
Attackers know what to attack before the election.

Precinct Voting
Analysis: Network Voting + Microfilm Ballots



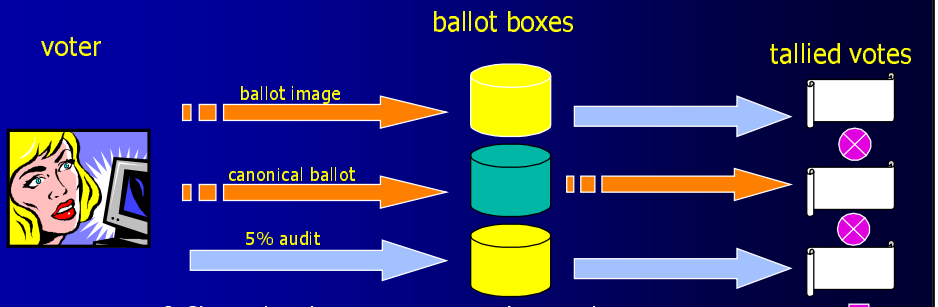
3 Channels: Electronic + Network + Microfilm

If one channel disagrees, the system may still be determinate. ?

The solution comes from the system itself.
Still based on a priori policy, but attackers now have to attack two processes.

Precinct Voting

Analysis: Network Voting + Real-time Auditing



3 Channels: Electronic + Network + Real-time Auditing

If one channel disagrees, the system may still be determinate.

?

The solution comes from the system itself.

Still based on a priori policy, but attackers now have to attack two processes.

Voting System Components

1. Voter Registration
   - Voter must be legally identified
2. Voter Authentication
   - Authenticate voter, ballot style and ballot rotation
3. Voting Station
   - Privacy and security
4. Ballot Box
   - Ballot integrity
5. Tallying and Auditing
   - Anonymity, Secrecy, Verification, Public proofs

Main Voting System Components

Voter Authentication

Authenticate voter, ballot style and ballot rotation

Voting Station

Privacy and security

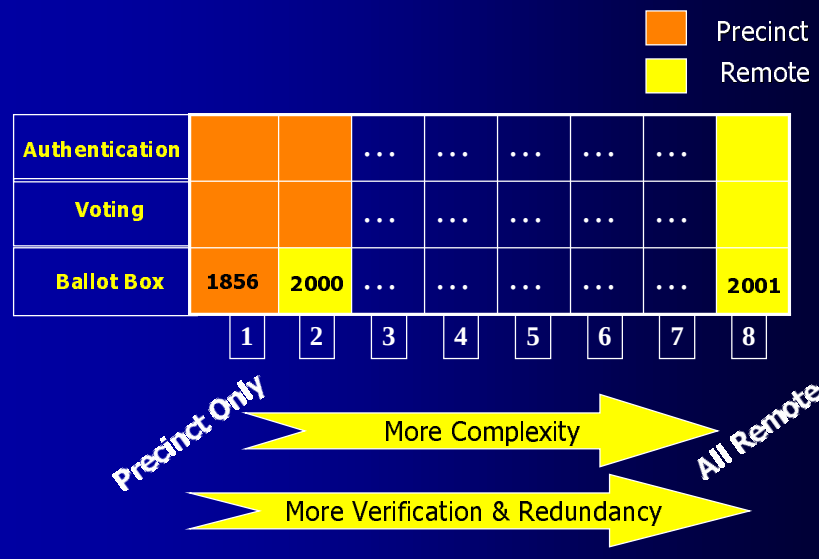
Ballot Box

Ballot integrity

Voting System Component Classification

Local or Remote

Voting System Classification



Who Let the Dogs Out?

" On the Internet, nobody knows you're a dog."
"Denial of Service has no solution."
"Computers are never secure."
"We need paper proof."
...

Precinct Electronic Voting

- Demonstrated at California Voting Technology Expo 2001.
- Challenges met (from current DRE systems):
  - reduce cost
  - increase number of vendors, keep uniformity
  - increase voting reliability (the "vote gap" issue)
  - reduce obsolescence, promote extensibility
  - authenticate voter and ballot style without hardware token (uses DVCs) http://www.safevote.com/aboutus.htm
- Solution: DELTA™
  - Safevote, software-only DRE
  - Intel, motherboards & architecture
  - Samsung, touch-screen & printers
  - Smart, write-once memory card (local ballot box, for ballot images)
  - Colfax International, integration (premier Intel Solution Provider)
  - Vendors can join and assemble their own systems

Reduces entry barrier for new vendors. Uses trained workforce – PC-based.

Precinct Internet Voting

- Used in November 2000, Contra Costa County, CA
  interim report at http://www.safevote.com/contracosta/
- Challenges met (from list of "impossibles"):
  - Uses stealth, moving target technology to forestall, with reliability as close to 100% as desired, the following attacks on the precinct Internet node:

Denial-of-Service	Large Packet Ping
Buffer Overrun	TCP SYN Flood
IP Spoofing	TCP Sequence Number
IP Fragmentation	Network Penetration

    http://www.safevote.com/tech.htm
  - authenticate voters and ballot style without hardware token (uses DVCs)
  - allow voters to verify on the Internet that their vote was received and is valid
  - support fail-safe privacy (even if everything fails and everyone colludes)
  - increase voting reliability (the "vote gap" issue)
  - reduce obsolescence, promote extensibility
  - voter freedom – vote from any precinct in the state
- Solution: DELTA-NET™
  - DELTA, with precinct network linked to the Internet by dial-up router.

Remote Internet Voting

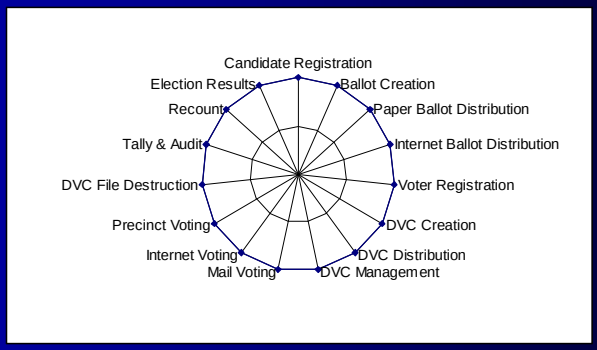
- Not for today in US public elections – need to test, test, test
- To be tested April/May 2001 at Umeå University Student Union, Sweden
- Financed and supervised by the Swedish Ministry of Justice, Foundation for Knowledge, Umeå County, and the University. Cooperation with the Swedish Post.
- Challenges being met (from list of "impossibles"):
  - Forestall attacks on the remote voter's machine – if the voter follows the voting instructions:

Spoofing (99.7%)	Man-in-the-middle (99.7%)

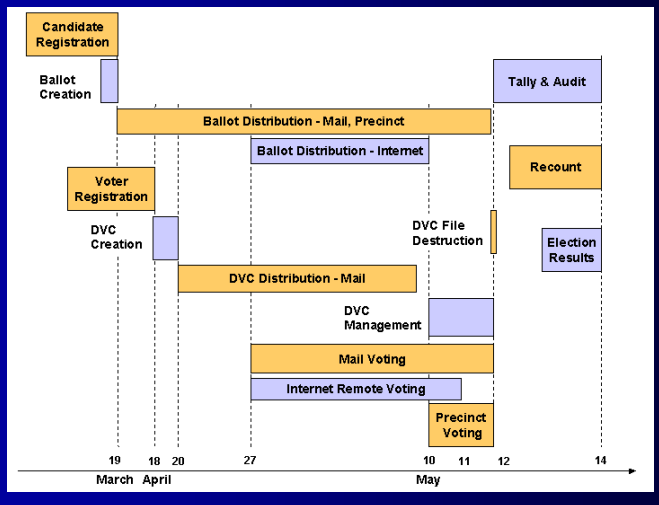
    (to be reported in The Bell, at http://www.thebell.net/archives/thebell2.3.pdf)

Virus (?)	Trojan-horse (?)
  - Forestall coercion and vote selling.
  - authenticate voters and ballot style without hardware token (uses DVCs)
  - allow voters to verify on the Internet that their vote was received and is valid
  - support fail-safe privacy (even if everything fails and everyone colludes)
  - increase voting reliability (the "vote gap" issue)
- Solution:
  - Read 59-page report at http://www.us.umu.se/arkiv/public.pdf

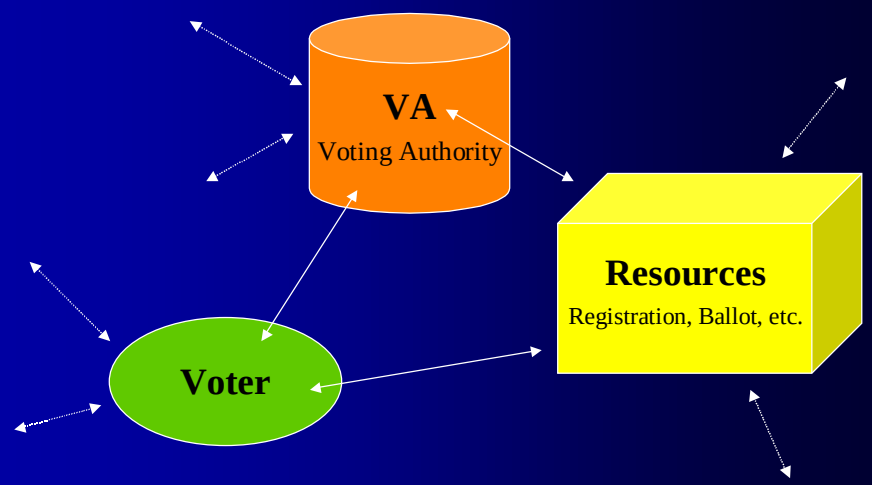
Election System - Phases



Election System - Time



Safevote: Multi-Party™ Protocol (example)



Open Standards: IVTA

- Safevote is a co-founder of the IVTA – http://www.ivta.org
- The Internet Voting Technology Alliance includes:
  - Companies
  - Universities, private and public research centers
  - Individuals
  - Government sectors
- The IVTA is an Internet standards setting body specific for voting applications, including public elections, that:
  - Offers open participation
  - Provides for unification of standards without integration
  - Uses peer public review procedures with public Workgroups
  - Provides protocol certification according to IVTA standards
  - Is a non-profit corporation, including all participants.
  - Not a vendor association!

16 Strict Voting System Requirements

http://www.thebell.net/papers/vote-req.pdf

1. ***Fail-safe voter privacy – the inability to link a voter to a vote***
2. ***Collusion-free vote secrecy – the inability to know the vote***
3. ***Verifiable election integrity –*** the inability to change the outcome except by properly voting

4. ***Fail-safe privacy in verifiability***
5. ***Physical recounting and auditing***
6. ***100% accuracy***
7. ***Represent blank votes***
8. ***Prevent overvotes***
9. ***Provide for null ballots***
10. ***Allow undervotes***
11. ***Authenticated ballot styles***
12. ***Manifold of links –*** avoid single points of failure even if improbable
13. ***Off-line secure control structure***
14. ***Technology independent***
15. ***Authenticated user-defined presentation***
16. ***Open review, open code***

Open Dialogue: THE BELL

- Safevote publishes THE BELL – http://www.thebell.net
- THE BELL:
  - A non-partisan monthly newsletter
  - Independent Editorial Board
  - Published in PDF and in print – searchable HTML next
  - Free subscription for PDF
  - 16 pages with quality information
  - Open peer reviewed articles – anyone may publish, only requirement is quality
  - Media Watch section – provides an easy collection of relevant news
  - Distributed worldwide
  - Public and Private sectors participate
  - Helps create the market
  - Helps find partners
  - Helps develop trust

Safevote Technology

USPTO Patent pending

- Secure Network Voting System
- Automatically Generating Unique, One-Way, Compact and Mnemonic Voter Credentials that Support Privacy and Security Services
- A High Entropy Encoding System for Network Voting
- Secure Network Voting System with Remote Voting
- System for Detection and Prevention of Denial of Service Attacks in Precinct-based Network Voting
- ...more

Summary of References

Voting System Requirements:
http://www.thebell.net/papers/vote-req.pdf

Specifications, demos, test results:
http://www.safevote.com

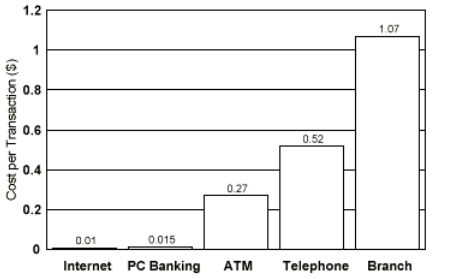
Contra Costa County Shadow Election, 2000:
http://www.safevote.com/contracosta/

Umeå University Union, Sweden, 2001:
http://www.us.umu.se/arkiv/public.pdf

Preventing Network (including DoS) and Data attacks:
http://www.safevote.com/tech.htm

Cost

Figure 8. Internet Banking is Cheaper for Banks



Source: Booz-Allen & Hamilton

Cost

Per Vote Cost Data

	Shareholder.com	ADP
Mail proxy card	$.36	$.34
Telephone vote	$.17	$.18
Internet vote	$.05	$.03

Corporations that receive a single, bundled charge for all services provided by their transfer agent may not be aware of per vote cost segmentation for registered shareholders.

Figure 7. Cost to Process Airline Tickets

$8.00: Travel agent books, using computer reservation system
$6.00: Travel agent books direct with airline
$1.00: Customer books "electronic ticket" direct with airline

Source: Air Transport Association of America, 11/20/97

What Voters Want

Contra Costa County, Calif., November 2000 – 307 voters at the precinct

This page is not about increasing voter participation!
The issue here is voter preference.

Would You Use the Internet to Vote:

- 60% would vote from home
- 34% would prefer to vote from the workplace
- 5% would prefer to use the Internet to vote at precincts
- 1% did try the system even though they declared they were completely opposed to the idea of Internet voting

Voters want so much to vote at home or office that several Internet and security experts have to continuously try to block their enthusiasm.

The advance of Internet voting in the private sector (legal in 28+ states) cannot be used as a justification for using it the public sector.

SAFEVOTE℠

Voting Systems: From Art to Science

Voting Technology Conference 2001
Pasadena, Calif., March 30-31
Caltech/MIT

Ed Gerck, Ph.D.
egerck@safevote.com
CEO & VP of Technology