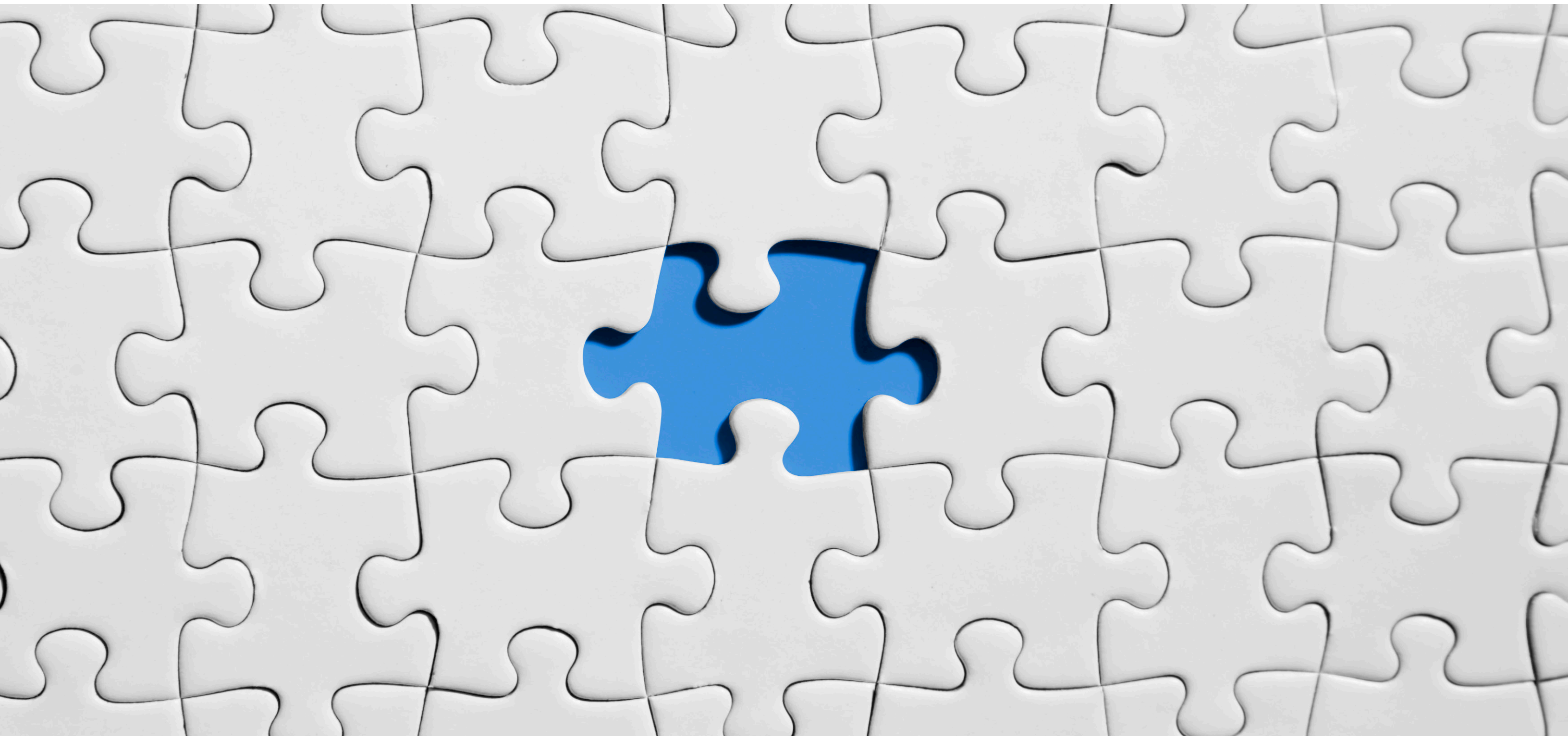
CAN TECHNOLOGY RESHAPE AMERICA'S ELECTION SYSTEM?



Bruce Yellin

Bruceyellin@yahoo.com

Knowledge Sharing Article

The Dell Technologies Proven Professional Certification program validates a wide range of skills and competencies across multiple technologies and products.

From Associate, entry-level courses to Expert-level, experience-based exams, all professionals in or looking to begin a career in IT benefit from industry-leading training and certification paths from one of the world’s most trusted technology partners.

Proven Professional certifications include:

- Cloud
- Converged/Hyperconverged Infrastructure
- Data Protection
- Data Science
- Networking
- Security
- Servers
- Storage
- Enterprise Architect

Courses are offered to meet different learning styles and schedules, including self-paced On Demand, remote-based Virtual Instructor-Led and in-person Classrooms.

Whether you are an experienced IT professional or just getting started, Dell Technologies Proven Professional certifications are designed to clearly signal proficiency to colleagues and employers.

Learn more at www.dell.com/certification

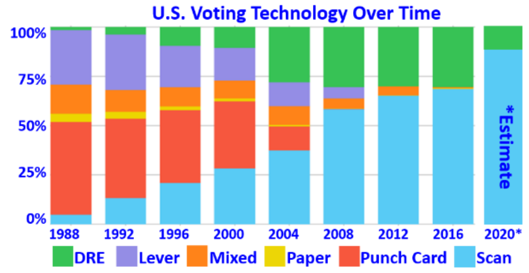
Table of Contents

Disclaimer: The views, processes or methodologies published in this article are those of the author. They do not necessarily reflect Dell Technologies' views, processes or methodologies.

Democracies are built upon the guarantee of free and fair elections, and in the United States, most candidates are elected to office by popular vote. Voting system technology seems simple, but it is anything but that. Those in favor of computer-assisted voting include election officials who appreciate the efficiency offered by electronic voting and citizens who enjoy smartphone simplicity. Skeptics, including IT experts and other citizen groups, are concerned about the safeguards that locally assembled and operated highly decentralized systems offer candidates.

Many of the election system challenges are attributable to the U.S. principle of states' rights. There is little agreement on the methods or ballots used by over 160 million voters who live in over 10,000 election jurisdictions of states, territories, villages, towns, cities, counties, districts, and areas.[1,2,3] As long as states meet their Constitutional obligation to hold the election, they are generally free to run them as they see fit. They design their databases, create rules for mail-in ballots, decide on in-person ID requirements, and other implementation issues.[4] For example, Wisconsin alone has 1,850 cities, towns, and villages that run their own elections.[5]

Leading up to the 2020 election, voters felt e-voting could improve access and ease administration. However, the pandemic put a wrench in the e-voting effort and it became a topic of debate. As a result, paper ballots made a comeback, harkening back to the days of Grover Cleveland's 1892 Presidential election.[6]



Every four years, according to the Constitution's Article II, Section 1, the presidential choice is decided by a group of Electoral College "electors" and not directly by citizens. Each state gets a minimum of three electors based on two Senators and at least one Congressperson. The College has a current maximum of 538 electors. In 48 states and Washington, D.C., the top vote-getter gets all the state allocated electoral votes, while Maine and Nebraska allocate as a percentage of the popular vote. A candidate earning 270 electoral votes is announced in mid-December as the next President and sworn into office on January 20 of the following year.

While the popular vote on election night often signals who will be the new President, in 2016, Hillary Clinton received nearly 3 million more votes than Donald Trump (2.1% difference) but lost the electoral college vote 227 to 304 giving the presidency to Trump.

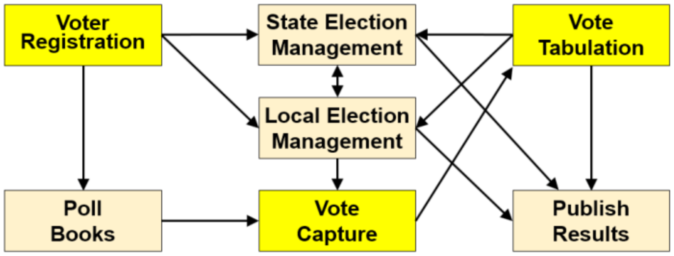
As systems become complex, they can become prone to unintentional error and subject to manipulation. In the IT world, safeguards such as firewalls and backups protect against something going wrong or having severe implications. The most common form of election safeguard is an auditable paper trail. With so many votes cast, even the slightest percentage of error when counting ballots can impact an outcome.

In the time between elections, the Voter Registration Database (VRD) must be maintained, equipment purchased, staff trained and coordinated, and voter education materials created. In the days, weeks, and months leading up to an election, these paper and electronic systems have to be designed, configured, and/or programmed to allow the voter to easily state their intention and for administrators to accurately record those intentions on Election Day.

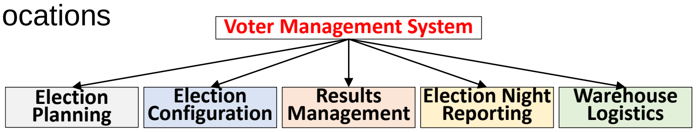
This paper is about the challenges faced by IT voting systems and what can be done to improve them. NOTE: The election community's rich set of acronyms are listed at the end of the paper.

General Election Architecture

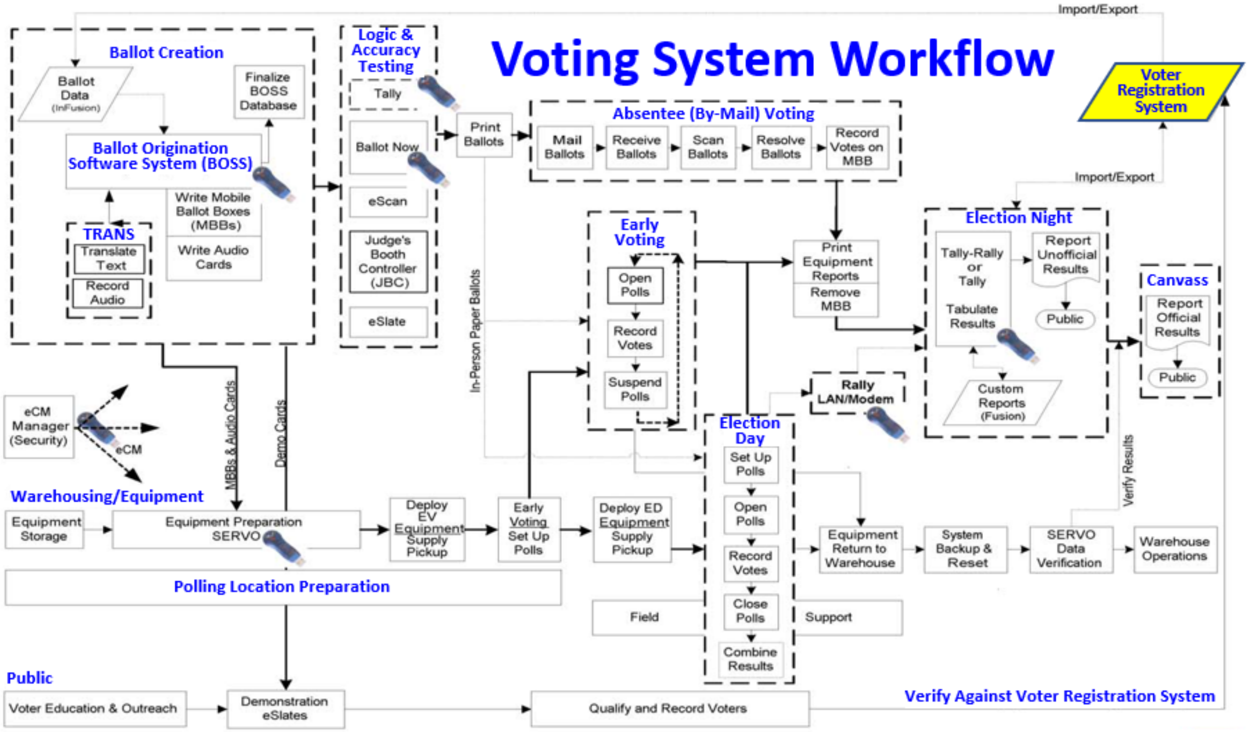
With a myriad of election systems and configurations found in the United States, this section focuses on the basic "Voter Registration", "Vote Capture", and "Vote Tabulation" components.[7]



Many jurisdictions leverage computer technology to run an election and begin the process with a supplier's overarching **Voter Management System** (**VMS**). A **VMS** contains guided methods to help election officials with candidate nominations. Based on a VRD of eligible voters, it also assists with ballot creation, printing, addressing, and mailing. The **VMS** helps program precinct equipment, coordinate logistics for polling locations and workers, tabulate precinct and central mail-in results, and final results reporting.



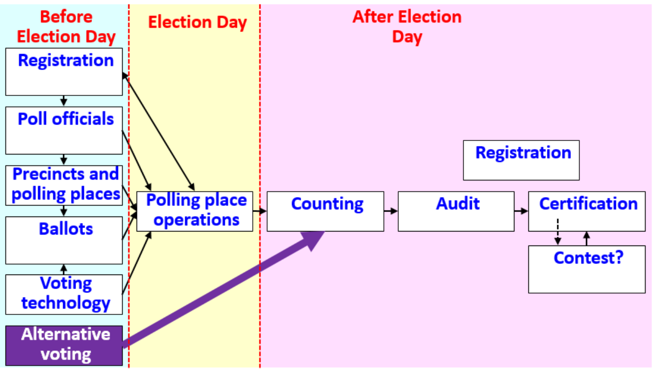
For the most part, components utilize Commercial-Off-The-Shelf (COTS) packaged products such as standard Dell servers, hyperconverged platforms, Oracle or Microsoft databases, Cisco networking equipment, VMware and Hyper-V virtualization, AWS cloud implementations, and so forth, allowing engineers to focus on election design elements while relying on commercial hardware and software support. Depending on a jurisdiction's level of modernization, component duplication at the state and local level can provide backup or disaster recovery. While state and county election boards try to have a modern infrastructure, older gear is often commonplace as replacement funding is often lacking. The following general **Voting System Workflow** depicts some of the processes of running an election in one jurisdiction.[8]



Funding greatly impacts the resources needed to keep up with voter demand on days leading up to and on Election Day, often manifesting itself in long precinct lines. In Texas, Harris County serves Houston's ~2.4 million voters with over 8,000 HART eSlate Direct-Recording Electronic (DRE) voting machines while Dallas County's 1.3 million voters use 4,000 ES&S ExpressVote Ballot Marking Devices.[9] These counties exemplify the various systems in simultaneous use on Election Day.

2018	Maker	Type	Model	QTY
Harris County	HART	DRE	ESLATE	8,189
	HART	DRE	JBC	2,072
	HART	DRE	DAU	1,940
	HART	Scanner	Kodak 1-660	8
Dallas County	ES&S	Ballot Mark	ExpressVote	4,000
	ES&S	Scanner	DS200	1,000
	ES&S	DRE	DS850	2

There are numerous subsystems in a typical election system, and jurisdictions tend to implement these interrelated functions differently.[10] Election Day is typically the culmination of twelve months of preplanning. This illustration shows the three major phases of election preparedness, with much of the functionality focused on the next election, while **alternative voting** handles absentee ballots typically after the polling place operations close. Jurisdictions that permit early voting, perhaps weeks before the official Election Day, are part of the Election Day process.

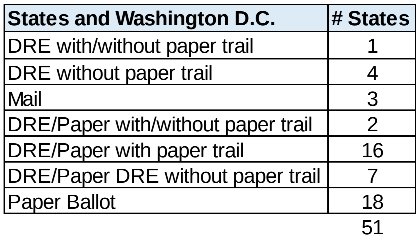


Voter Registration Database

The Constitution of 1789 does not specify who can vote.[11] That job was left to individual states, and hundreds of years ago, that generally meant white male landowners 21 and older could vote. These days, every U.S. citizen 18 years and older that meets individual state regulations is eligible to vote after registering through a state or local registration system.

The VRD is just one piece of the registration system. Elections are complex and often present themselves as a logistical nightmare. There are roughly 330 million Americans and 75% of them are 18 years and older. Of those eligible, ~64% register to vote and appear in a local VRD.[12] A VRD has many uses, among them is to create an accurate list of those ~160 million voters. It also contains other federally suggested election metadata as implemented by state and local entities such as a voter signature and other identification that permits voters to vote at a polling place or by mail.

The U.S. has many individual VRDs in use. In 2016, 38 states had individual systems. In Texas, 215 counties use the state system and 39 counties had their own VRD.[13] In the U.S., these systems support more than 10,000 voting jurisdictions and 1.4 million poll workers with over 800,000 voting machines that in some way capture a vote as shown below.[14,15,16] Not only can equipment vary by jurisdiction, the basic functionality of the equipment can differ. For example, some states using DREs can produce a paper audit trail while others cannot, and other jurisdictions support DRE machines and paper ballots.



States and Washington D.C.	# States
DRE with/without paper trail	1
DRE without paper trail	4
Mail	3
DRE/Paper with/without paper trail	2
DRE/Paper with paper trail	16
DRE/Paper DRE without paper trail	7
Paper Ballot	18
	51

The registration database's primary use is to generate paper and electronic poll books of voters allowed at a particular precinct and for absentee/mail-in ballot processing. It includes a voter's address, registration form signature, and whether they already submitted a ballot. Some jurisdictions update or journal the database's signature entry when a voter signs the poll book. The VRD also maintains political party affiliation to aid officials in staffing primary elections.

The general steps of processing a mail-in or absentee ballot include:[17]

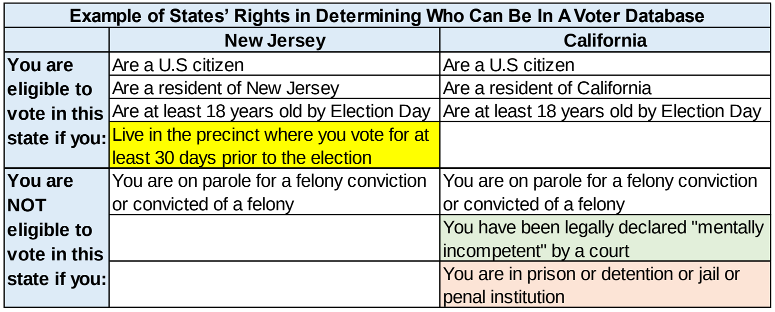
1. Ballots received are pre-processed, preparing them for counting before Election Day. Wisconsin, Pennsylvania, and parts of Michigan begin on Election Day.
2. Barcoded outer envelopes are scanned and checked to see if the voter already voted.
3. Jurisdictions with outer envelope signatures and addresses are cross-checked.
4. "Problem envelopes" can be submitted to a cure process allowing for voter remediation.
5. Outer envelopes are sorted by precinct and can be alphabetized for a VRD check.
6. The ballot is removed from the outer (and optional inner) envelope by hand or machine.
7. Ballots are flattened and examined before scanning, trying to prevent scanner jams.
8. Salvageable damaged ballots can be hand-transcribed to a fresh ballot.

9. Ballots are scanned.
10. The results are tabulated and announced.

The registration database is part of an all-encompassing system involving numerous uni- and bidirectional secure federal, state, and local data feeds as well as from citizens and other electronic sources. The 2002 Help America Vote Act required states to establish a statewide VRD and verify voter accuracy by comparing it to other state records.[18]

The VRD helps estimate voter demand at a precinct allowing officials to adjust staffing levels. Voters can also check their data for accuracy. As an anti-fraud measure, the database helps prevent voters from voting twice. Many VRD design goals were specified by the Association for Computing Machinery to help unify each state's approach to their system.[19]

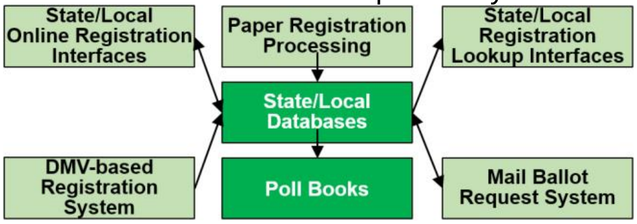
In all jurisdictions, voter registration is an IT function critical to safeguarding free and fair elections. To ensure democracy's spirit of "one person, one vote", each state is authorized to track voter eligibility. This simple example shows that New Jersey's rules are different from California's. Each system requires secure data feeds from other state or federal agencies just to maintain these simple rules.



Example of States' Rights in Determining Who Can Be In A Voter Database

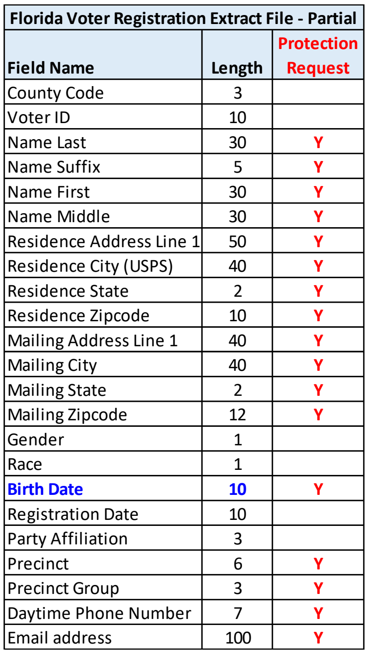
	New Jersey	**California**
You are eligible to vote in this state if you:	Are a U.S citizen	Are a U.S citizen
	Are a resident of New Jersey	Are a resident of California
	Are at least 18 years old by Election Day	Are at least 18 years old by Election Day
	Live in the precinct where you vote for at least 30 days prior to the election	
You are NOT eligible to vote in this state if you:	You are on parole for a felony conviction or convicted of a felony	You are on parole for a felony conviction or convicted of a felony
		You have been legally declared "mentally incompetent" by a court
		You are in prison or detention or jail or penal institution

A great deal of VRD activity is attributed to maintaining eligible voter lists by purging ineligible citizens through intra-database data exchanges. The process requires automation as some systems contain millions of voter records. Ineligible names are removed or updated by an address change in the Post Office National Change of Address (NCOA) database, state Department of Motor Vehicle (DMV), or state tax collection authority. Death notifications, such as from Florida's Department of Health and Vital Statistics, or state stipulated murder or sexual offense disqualifications such as from a Kentucky Department of Corrections data feed must be tracked. Thirty states also use a data feed from the Electronic Registration Information Center, a non-profit organization that helps states improve the accuracy of voter rolls.[20]


State/Local Online Registration Interfaces
Paper Registration Processing
State/Local Registration Lookup Interfaces
State/Local Databases
DMV-based Registration System
Poll Books
Mail Ballot Request System

As shown by the chart above, flexibility is a critical element of a registration database. The Federal government can only make recommendations for interoperability, and state and local administrators must work with other states and municipalities to exchange and incorporate data from other systems. The nature of the system's uniqueness may dictate that data exchange is through a physical CD-ROM or DVD, or a communications link. Data exported from a system must have security controls and imported data may require an Extract, Transform, and Load (ETL) process if the data is “dirty” or reformatted for database compatibility reasons.

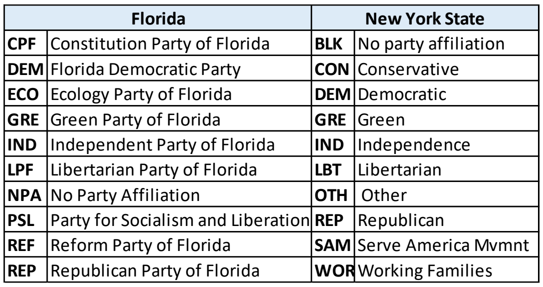
While a common state goal is for seamless data exchange, systems must allow for non-uniform format ETL data conversion operations such as when data is exchanged between Florida and New York. This abbreviated portion of Florida’s file layout to the right shows a 10-character **Birth Date** MM/DD/YYYY. New York State maintains the birth date as 8 characters YYYYMMDD.[21]



Florida Voter Registration Extract File - Partial

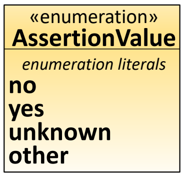
Field Name	Length	Protection Request
County Code	3	
Voter ID	10	
Name Last	30	Y
Name Suffix	5	Y
Name First	30	Y
Name Middle	30	Y
Residence Address Line 1	50	Y
Residence City (USPS)	40	Y
Residence State	2	Y
Residence Zipcode	10	Y
Mailing Address Line 1	40	Y
Mailing City	40	Y
Mailing State	2	Y
Mailing Zipcode	12	Y
Gender	1	
Race	1	
Birth Date	**10**	Y
Registration Date	10	
Party Affiliation	3	
Precinct	6	Y
Precinct Group	3	Y
Daytime Phone Number	7	Y
Email address	100	Y

Other differences that must be accounted for include Florida’s 30-character last name while New York uses 50 characters. Common fields can also have different meanings, allowing a state to define a unique layout. States can permit voters to declare some of their information is **private** such as their **name** and **address**, while fields such as gender, race, and party affiliation are deemed public information. To the left, these two states also have unique party affiliation abbreviations.

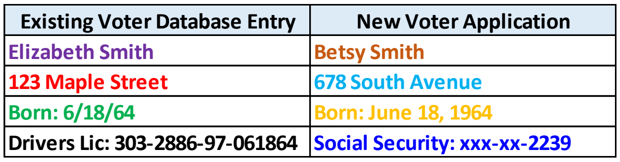


Florida		New York State	
CPF	Constitution Party of Florida	**BLK**	No party affiliation
DEM	Florida Democratic Party	**CON**	Conservative
ECO	Ecology Party of Florida	**DEM**	Democratic
GRE	Green Party of Florida	**GRE**	Green
IND	Independent Party of Florida	**IND**	Independence
LPF	Libertarian Party of Florida	**LBT**	Libertarian
NPA	No Party Affiliation	**OTH**	Other
PSL	Party for Socialism and Liberation	**REP**	Republican
REF	Reform Party of Florida	**SAM**	Serve America Mvmnt
REP	Republican Party of Florida	**WOR**	Working Families

Given the importance of exchanged data to voting integrity, the Federal Government established a standard NIST data dictionary to assist election IT developers in reducing the data conversion burden.[22] Using a baseline common data format, future enhancements include the ability to match state driver license numbers. A Federal Unified Markup Language model defined the necessary Extensible Markup Language (XML) and JSON schemas to facilitate easier data exchanges such as the AssertionValue Enumeration and definitions of “no”, “yes”, “unknown”, and “other”.



Adding new voters or updates to database records are triggered by a new registration form, another database feed such as a released convict that is permitted to vote, a driver passing their road test and checking off a DMV box requesting registration, driver’s license renewal, and more. Care is taken to ensure unique entries are maintained and not duplicated. In the data processing world, algorithms aid list comparison, but the task is still complex. For example, determining that **Elizabeth Smith** and **Betsy Smith** (Betsy is a nickname) at these addresses is or isn't the same person can require additional matching such as from the DMV or Social Security Administration records.



Existing Voter Database Entry	New Voter Application
Elizabeth Smith	Betsy Smith
123 Maple Street	678 South Avenue
Born: 6/18/64	Born: June 18, 1964
Drivers Lic: 303-2886-97-061864	Social Security: xxx-xx-2239

Examples of algorithm matching include a full character name match and Soundex, which is a phonetic match for names that are pronounced the same. These approaches are not perfect, as in the case of "Smith", "Smyth" and "Smythe", which all share the same Soundex "S530" code.

If a data match cannot be established, human intervention may be needed. In our example, **Betsy** at **Maple Street** may have moved to **South Avenue** and mistakenly filled out a new voter application with her nickname instead of a change of address notification with her birth name.

Algorithms can also attempt to find matches based on incomplete information. For instance, the last name mismatch of **Elizabeth Smith** at **123 Maple Street** could show an NCOA entry for Jim Kirk at that address, requiring further investigation. Perhaps **Elizabeth** and Jim both reside at that address. A match of **Elizabeth Smith** and **Elizabeth** J. **Smith** at that address could imply one data feed had a middle initial or is a close relative of **Elizabeth's** who uses a middle initial at that address. An administrator can always try to reach out to the voter for clarification.

The same database could be scanned for jury duty candidates, or interstate matching to find voters registered in two states. It can also assist homeless voters with an entry indicating their mailing address, such as a relative's house, is physically different from where they live.

Database matching is a vital administration tool and must precisely follow a rule base. For example, voter names can have a wide variance, such as a nickname or maiden name on various forms of identification. Stored signatures must be processed for allowable variances through alternate signatures, multiple versions of a signature, and illegible signatures since signature matching is an inexact science. An administrator can often assist a database match when confusion arises, especially when the administrator brings years of expertise to bear.

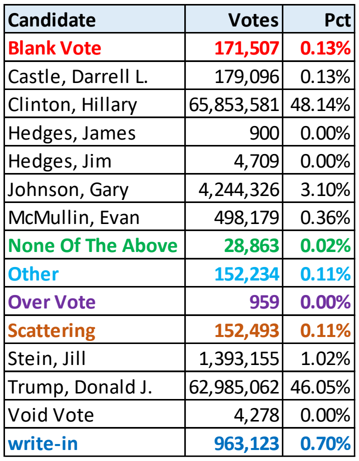
Purging Data Records

Record purging can be error-prone given the databases' volume of daily change. Incorrectly culling ineligible voters disenfranchises them, while not identifying them threatens voting integrity, such as if they move to another state and vote in both state elections. Applying increased eligibility criteria could result in less purged records, while fewer data checks could purge too many voters. False-positive purges are bad while a false negative purge could erroneously keep a citizen on the VRD. To improve transparency, reduce errors, and prevent unauthorized database access, some states try to notify voters they are being purged.[23]

Failing to purge records of the dead are part of the alleged 1960 fraud under Chicago Mayor Daley. Many believe but never proved he arranged for dead voters not yet removed from the manual system to cast ballots for John Kennedy.[24] There were also reports of ballot-box stuffing under his watch, that in total, allowed Kennedy to win Illinois by a slim 8,858 votes (0.2%).[25,26]

Automated record purging makes it prudent to have an audit trail and secondary confirmations through alternate methods. For example, to determine a voter has moved, an administrator should check with at least two databases such as NCOA and their current state's DMV. With the possibility of human error or unauthorized access, VRD data must also be verifiable as well as encrypted to safeguard privacy for driver's license numbers, birth dates, etc. Voting commissions should provide tools such as New Jersey's Division of Elections portal to allow voters to verify their registration information.[27] Independent verification and audit trails aid in reversing intentional and unintentional entries. Auditable data should be generated any time a record is created, deleted, or modified, the database undergoes configuration changes, security policy changes, or the design layout is altered. It helps to have the audit trail in a separate data medium such as paper or an air-gapped tape backup device (an electronically disconnected and isolated data copy rather than, for instance, an online cloud backup).

The VRD is a Single Version Of Truth in business management terms – a central database of every legal voter in a consistent and concise form. Each record follows a published layout and contains other data that makes it easy for a state to publish public extracts.[28]



Candidate	Votes	Pct
Blank Vote	**171,507**	**0.13%**
Castle, Darrell L.	179,096	0.13%
Clinton, Hillary	65,853,581	48.14%
Hedges, James	900	0.00%
Hedges, Jim	4,709	0.00%
Johnson, Gary	4,244,326	3.10%
McMullin, Evan	498,179	0.36%
None Of The Above	**28,863**	**0.02%**
Other	**152,234**	**0.11%**
Over Vote	**959**	**0.00%**
Scattering	**152,493**	**0.11%**
Stein, Jill	1,393,155	1.02%
Trump, Donald J.	62,985,062	46.05%
Void Vote	4,278	0.00%
write-in	**963,123**	**0.70%**

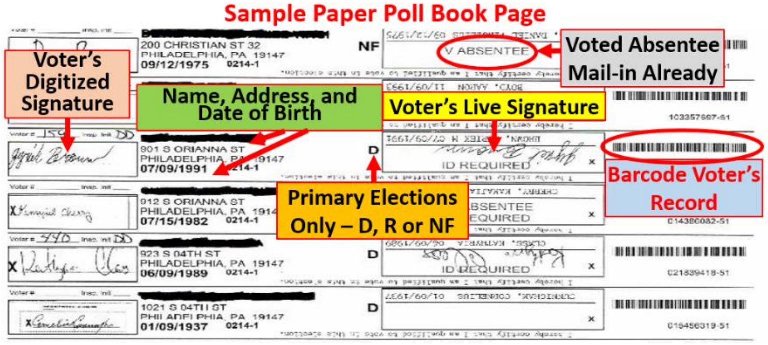
Data from VRDs and other public databases (that may restrict the use of private information) is turned into an insightful demographic analysis of how America truly votes. Harvard's Dataverse extract of the 2016 U.S. Presidential race shows almost 6% of U.S. voters did not vote for either Clinton or Trump.[29] Over **171,507** voters, representing **0.125%** of total votes, submitted a **blank ballot**, which is different than **28,863** voters who selected "**None Of The Above**", **152,234** "**Other**", **959** for "**Over Vote**" (when a voter makes more than one entry per row), **152,493** for "**Scattering**" (write-in votes for unregistered candidates), and **963,123** voters than may have chosen a "**write-in**" candidate. Voters also picked "James Hedges" 900 times in Colorado and Mississippi while "Jim Hedges" of Arkansas received 4,709 votes (there is a James "Jim" Hedges who ran for the Prohibition Party in 2016, but from a legal ballot perspective, the actual name must be precise.)[30]

Most of the political parties chosen included the popular Democrat, Republican, Independent, Libertarian, and Green, while some of the parties represented by candidates included "We The People", "Approval Voting Party", "Legal Marijuana Now", and "Nutrition Party". Given the 2016 popular vote victory margin between Clinton and Trump was close, and the electoral vote ran opposite of the popular vote, we can speculate that a pared-down list of available candidates could have refocused an additional 2.3 million voters and changed the Presidential outcome.

VRD's use COTS componentry and are subject to the same malware risks and network attack threats of any desktop computer. Most equipment uses close source code and is subject to non-disclosure agreements, so it is unclear what the processing algorithms are doing. As more equipment is added to a network, its potential exposure profile increases. This is especially true of precincts relying on wireless internet access making encrypted communications mandatory. Access control and authentication issues can also arise given the number of poll workers that use the equipment. The nature of distributed networks requires extra care to ensure proper backups, rollback-recovery, and auditable capabilities are built into the system.

Poll Books

Poll books are created from VRD extractions just before an election to create a digital or paper list. The list allows poll workers to record a voter signature during the Election period. Paper records such as the example to the right are from a binder of sheets printed for that particular jurisdiction's polling station. There are places for the signature, which the poll worker uses to verify against their previously obtained digitized signature, and address, birth date, and party affiliation which is important during a primary election. If the voter already submitted an absentee ballot, it would be noted on this page, preventing them from voting a second time. Using their barcode for the VRD record identifier, their current live signature can also be captured and likely used for the next election.


Sample Paper Poll Book Page

[redacted]
200 CHRISTIAN ST 32
PHILADELPHIA, PA 19147
09/12/1975 0214-1
NF
V ABSENTEE

Voter # 159 Insp. Init DD
[redacted]
901 S ORIANNA ST
PHILADELPHIA, PA 19147
07/09/1991 0214-1
D
ID REQUIRED
103357667-51

[redacted]
912 S ORIANNA ST
PHILADELPHIA, PA 19147
07/15/1982 0214-1
ABSENTEE
REQUIRED
014386082-51

Voter # 440 Insp. Init DD
[redacted]
923 S 04TH ST
PHILADELPHIA, PA 19147
06/09/1989 0214-1
D
ID REQUIRED
021839418-51

[redacted]
1021 S 04TH ST
PHILADELPHIA, PA 19147
01/09/1937 0214-1
D
015456319-51

Voter's Digitized Signature
Name, Address, and Date of Birth
Voter's Live Signature
Voted Absentee Mail-in Already
Barcode Voter's Record
Primary Elections Only – D, R or NF

An Electronic Poll Book (EPB) displays voter data for a particular station on a COTS console from a roster of eligible voters downloaded through a wired communications line, WiFi, or a USB thumb drive. Poll workers could be assisted by algorithmic comparison of the digitized and live signatures to analyze stylus speed, pressure, and other handwriting attributes. KNOWiNK's Poll Pad is an EPB tablet that can add precinct functions such as same-day registration.[31] Poll Pad uses WiFi/MiFi, AWS's GovCloud, and a custom database, and is deployed using the Cisco Meraki MDM that meets FIPS 140-2 and PCI DSS Level 1 security requirements.[32]

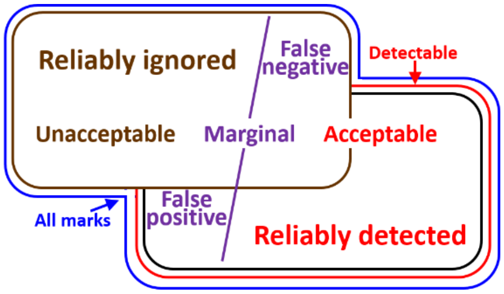
In some states, an EPB must be on a network to receive updates such as who might have voted in another precinct. In other states such as Michigan, voter data is local to the device and should not be on a network.[33] In general, all networked devices must be part of a secure communications initiative since it is a point of attack for a cyberterrorist intent on disrupting an election, possibly enabling a person to impersonate another voter, or serving as an entry point for a virus that could impact ballot tallies. As with any hardware/software combination, care would need to be taken that the equipment was not manufactured or updated with a virus. A computer virus can also infect the VRD through data modification and cause system-wide damage such as purging of valid voters or changing the final tally.

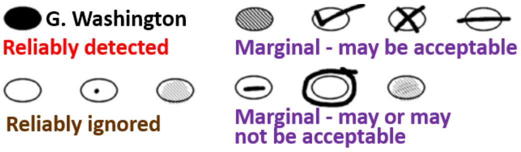
Casting a Vote

To date, there are four basic methods used to cast a vote. Two involve paper and two use machines. As with everything discussed, these methods vary by jurisdiction along with the layout of the paper forms and types of machines.

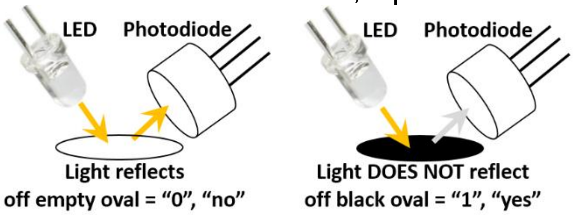
Paper Ballots – Large heavy-weight paper sheets designed with empty ovals, ellipses, boxes, and other shapes record a voter's choice when filled in with a **blue** or black pen, felt-tipped pen, or pencil. Any mark not in an oval or box is not read, so a voter who makes a mistake is unable to cross out or erase an entry, and shapes like crosses and checkmarks are discouraged. These ballots can be filled out at a polling place or even at home.

In this illustration of an optically read rounded rectangle, a detectable mark within the **red outline** can **reliably** be processed by the optical scanner as a positive assertion. Marks that fall outside this shape can yield unacceptable or unreliable results such as a **reliably ignored mark** not detected when scanned. **Marginal marks** may or may not be tallied as intended.



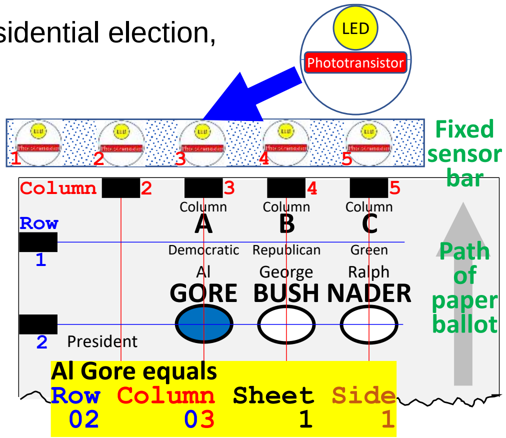

G. Washington
Reliably detected
Marginal - may be acceptable
Reliably ignored
Marginal - may or may not be acceptable

Similar to a barcode reader, Optical Mark Recognition (OMR) uses a photodiode to capture reflected LED light intensity from the oval's white or empty space ("0" or "no"). A black oval absorbs light, so none is reflected into the photodiode, which is translated into "1" or "yes".



Voting categories are arranged into a familiar grid of **rows** and **columns** that align with voting choices. In this hypothetical example from the 2000 Presidential election, there are three candidates – Al Gore, George Bush, and Ralph Nader. Each candidate is under their party headings that align under **columns 3, 4, and 5**, and the office they are running for is in **row 2**.

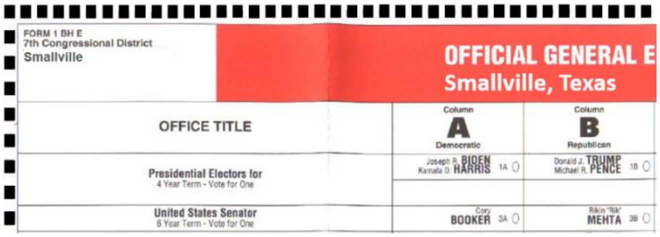
This **ballot page** is scanned by OMR that aligns the page optically as guided by **black rectangle** timing marks that intersect at preprinted **rows** and **columns**, ensuring the page is fed straight. If the page is crooked, the ovals will not line up under photodiodes, and choices will not be sensed and translated correctly.



Using the standard (**row**, **column**) array data structure, the three possible Presidential choices are located at coordinates Ballot (**2**,**3**), Ballot (**2**,**4**), and Ballot (**2**,**5**). In this example, a **ballot** passes under a **fixed sensor bar**, and Ballot (**2**,**3**) is translated into a "1" or "yes" for Al Gore, while Ballot (**2**,**4**) and Ballot (**2**,**5**) are translated into "0" or "no". The voter in this example filled in the **oval** at address "020311" as processed by the photodiodes. A page scan creates a matrix of values that represent the voter's wishes, and "no" votes can be discarded.

In this way, a standard scanner can be used for a page of names, categories, and questions that vary by jurisdiction and year. By aligning **row** and **column** timing tracks, a program "asks" a question and simple optics read a voter's choice. This concept is used for the entire ballot of officials and questions. A two-sided ballot uses a two-sided scanner.

Paper ballots like these, which may have been filled out at home weeks before election day, can be individually scanned at the polling place or batched processed by a high-speed scanner at the central election location. This is an example of a part of a New Jersey paper ballot for the 2020 election cycle.

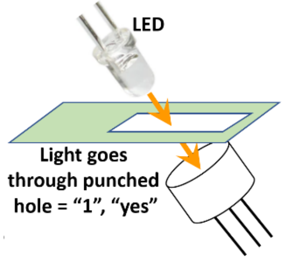


FORM 1 BH E
7th Congressional District
Smallville

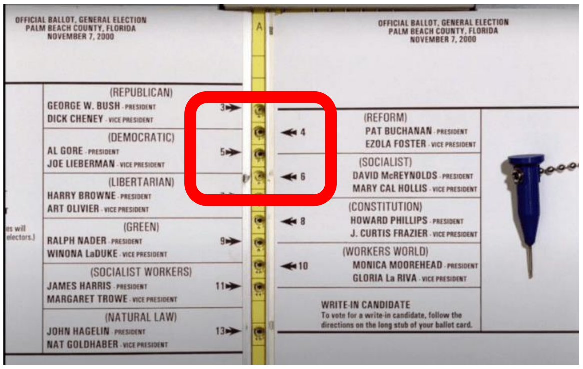
OFFICIAL GENERAL E
Smallville, Texas

OFFICE TITLE	Column A Democratic	Column B Republican
Presidential Electors for 4 Year Term - Vote for One	Joseph R. BIDEN Kamala D. HARRIS 1A ○	Donald J. TRUMP Michael R. PENCE 1B ○
United States Senator 6 Year Term - Vote for One	Cory BOOKER 3A ○	Rikin "Rik" MEHTA 3B ○

Paper Punch Cards – Phased out by 2014 because of their inability to reliably capture voter choices.[34] The premise is similar to a paper ballot. A hole at a particular row and column is translated as a positive selection when the LED light shining through it is received by a photodiode. If there was no selection made at that row and column, then there would be no hole and the light would not be detected by the photodiode, meaning a “0” or “no”.



While simple in concept, what happened in Florida’s Palm Beach County in 2000 was anything but. Using a punch card User Interface (UI), voters used a pointed tool to make a hole next to their choice in a “butterfly” ballot. The card was read by a high-speed reader at the central location. In this case, the punch card UI failed to prevent voter confusion and errors. Some voters ignored the instructions and black location arrow, making a hole next to both Presidential and Vice-Presidential names. Some voted for two candidates - Buchanan and Gore. Others voted for Gore by making a hole next to Buchanan. Nothing in this poor ballot design would help the voter catch their mistakes.[35]



OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

es will
electors.)

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT 3

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT 5

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT 9

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT 11

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT 13

A

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

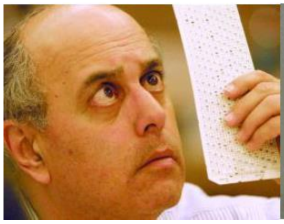
4 (REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

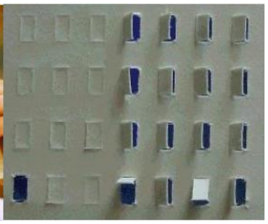
6 (SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

8 (CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

10 (WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

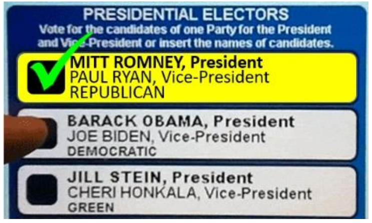
WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.





Some voters using the tool failed to fully punch out holes, creating “hanging chad” fragments that fouled up the automatic card reader. Many punch cards had to be reviewed by hand, leading to recounts that went on for weeks as some interpretations were difficult to make. Bush eventually beat Gore by 537 votes in Florida, marred by an election with a bad UI that may have changed history and certainly hurt our faith in the voting system.

Direct Recording Electronic (DRE) – A system incorporating a computer and usually a touchscreen that guided a voter through the voting process, ensuring they cannot vote outside administrator rules, such as accidentally voting for more than one Presidential candidate. In some machines, touching the space next to the candidate highlights the choice in yellow along with a **large green checkmark** ✓ . DREs became popular, in part, because of the drawbacks of paper ballots, such as the need to customize, multilanguage versions, large font versions, printing expenses, distribution to polling places, and storage after the election.



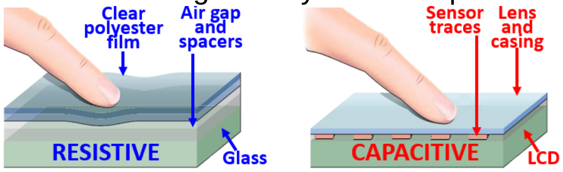
PRESIDENTIAL ELECTORS
Vote for the candidates of one Party for the President and Vice-President or insert the names of candidates.

☑ MITT ROMNEY, President
PAUL RYAN, Vice-President
REPUBLICAN

■ BARACK OBAMA, President
JOE BIDEN, Vice-President
DEMOCRATIC

■ JILL STEIN, President
CHERI HONKALA, Vice-President
GREEN

Touchscreens are a key piece of this solution and use **resistive** or **capacitive** technology.[36] ATMs and some tablets use pressure **resistive** pads that allow a finger or stylus to compress a conductive air-gapped plastic against conducting glass, making it ideal in harsh conditions such as wintertime when people wear gloves. **Capacitive** screens use the fingertip's skin as a conductor. In either case, the touchscreen surface has a grid of embedded electrodes. A completed circuit allows the screen controller to process the coordinates and pass them to the operating system. According to the Voluntary Voting System Guidelines (VVSG), a touchscreen must be usable by voters with prosthetic devices and not require direct bodily contact as part of the circuit, and if it does, a stylus must be provided.[37]



The DRE touchscreen can be multilingual, have different font sizes, and offer audio prompting. Voter choices are stored in the machine's memory. When the ballot is submitted, some DREs print a Voter-Verifiable Paper Trail (VVPT) receipt of selections, similar to a grocery receipt. When the polling station closes, a supervisor's master card allows the system to transmit results to a central site or save the results to removable media such as a USB stick, as well as generate an administrator VVPT audit printout in the event a recount is needed.

Some DRE systems serve as a Ballot Marking Device (BMD) and print out a marked paper ballot of the voter's choices. Using a multilingual UI, along with optional visual or audio prompts, they can assist with the voting process. DRE technology can also try to understand a voter's ballot intentions, and through an improved UI, remove voter confusion and create a positive experience. For example, a DRE could have prevented a Florida voter from both selecting Joe Biden for President and writing his name in the "Write-in Candidate" space. Some machines can create a Quick Response (QR) code or barcode for use by the central processing facility.

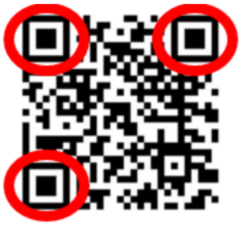
Older DREs had lever switches to record votes on mechanical counters. At election close, the counters were hand-copied and reported or generated a paper tape summarizing the counter totals. These machines may still be in use, but production has ceased and phased out in favor of other solutions.

Barcodes are a key coding technology that improves election speed, accuracy, and efficiency. Envelopes, paper ballots, VVPT, poll books, and more use barcodes to facilitate processing and tabulating. Invented in 1952, black and white bars absorb or reflect light into a photodiode using

OMR to generate a data string.[38] This barcoded receipt was printed by a voting machine summarizing the voter's choices and creating an auditing barcode of selections as shown inside the **red oval**.

Similar to Morse code's dots and dashes, and popular on grocery items, barcodes use a "1" and "0" code representing light absorbed (black) or reflected (white) stripes. Based on the code, the data is translated into a meaningful sequence that could contain voter choices or help postal machines route a ballot envelope to the proper mail carrier's route.

There are dozens of coding methods, but one of the more interesting ones is the QR code two-dimensional matrix such as this one.[39,40] Look closely and you will see three alignment squares highlighted in **red** that orient the QR code reader. QR codes can encode thousands of characters of data using the basic photodiode light reflection concept. A BMD's filled-out printed ballot often has a QR code that serves as a secondary summary of the voter's choices. QR codes also appear on candidate campaign literature allowing voters to scan them with their smartphone to get more information, such as a candidate's position on a particular issue.

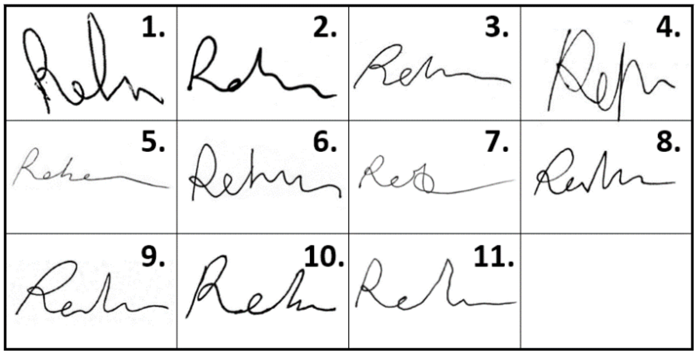


Verifying the Signature

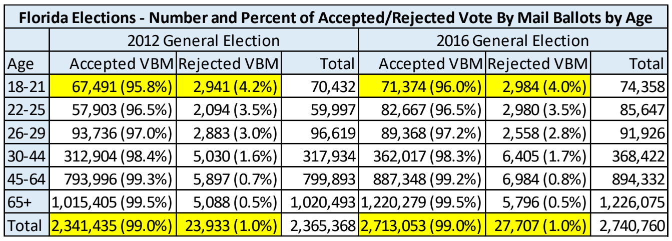
The coronavirus caused more voters to use mail-in ballots than ever before, moving signature verification responsibility from the poll worker to the central processing facility. As a result, even greater reliance on verification was needed to prevent impersonation of a legitimate voter. It is unlikely the impersonator knew what the previously-stored signatures looked like.

A signature is a key method in determining the voter's identity, even when a signature changes over time. Baseline signatures are stored during the registration process or updated during triggering events. Signatures can also be "versioned" with multiple vintage signatures kept on file. Over half the states use envelope signature matching to verify a voter's identity.[41]

Pretend you are an election official comparing an envelope signature against the VRD. Using a signature matching challenge issued by the NY Times, can you match two signatures? Make a note of your choices - the correct answer is found in the CONCLUSION section of this paper.



With Vote By Mail (VBM) ballots, trained officials compare an envelope signature against the signature(s) on file. In their judgment, if the two signatures are sufficiently similar, the ballot is accepted and counted. If the match is in doubt, the ballot is segregated for further consideration and not counted until the individual's identity can be verified. At the precinct, poll workers with typically less signature comparison training make the same judgment call. Years of training would be needed to turn workers into handwriting experts, so their training reaches a "middle ground." They are taught that if there is any doubt, then proceed as if there is no positive match.



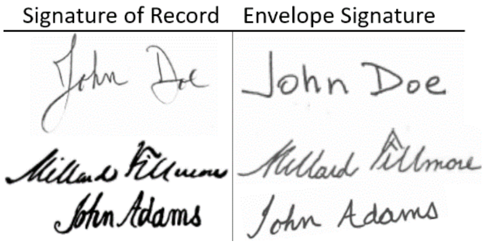
Florida Elections - Number and Percent of Accepted/Rejected Vote By Mail Ballots by Age

	2012 General Election			2016 General Election		
Age	Accepted VBM	Rejected VBM	Total	Accepted VBM	Rejected VBM	Total
18-21	67,491 (95.8%)	2,941 (4.2%)	70,432	71,374 (96.0%)	2,984 (4.0%)	74,358
22-25	57,903 (96.5%)	2,094 (3.5%)	59,997	82,667 (96.5%)	2,980 (3.5%)	85,647
26-29	93,736 (97.0%)	2,883 (3.0%)	96,619	89,368 (97.2%)	2,558 (2.8%)	91,926
30-44	312,904 (98.4%)	5,030 (1.6%)	317,934	362,017 (98.3%)	6,405 (1.7%)	368,422
45-64	793,996 (99.3%)	5,897 (0.7%)	799,893	887,348 (99.2%)	6,984 (0.8%)	894,332
65+	1,015,405 (99.5%)	5,088 (0.5%)	1,020,493	1,220,279 (99.5%)	5,796 (0.5%)	1,226,075
Total	2,341,435 (99.0%)	23,933 (1.0%)	2,365,368	2,713,053 (99.0%)	27,707 (1.0%)	2,740,760

At first glance, initial signature screening seems to work. However, the American Civil Liberties Union found between 2012 and 2016, racial and ethnic Florida minorities were more likely to have their mail ballots rejected for signature issues or a missing inner "secrecy envelope" and not have them cured (a process to correct a ballot's signature) when compared to the general voting population.[42] Younger voters were about four times as likely to have their ballot rejected and uncured. In 2016, 315,651 mail-in ballots were rejected for a variety of reasons, and with the 2020 projections, the number of rejected ballots could surpass one million.[43,44] Signature matching is a serious election issue, so more care is needed during this phase of vote processing, but judgment calls can be hard and time-consuming, and lead to increased voter suppression.

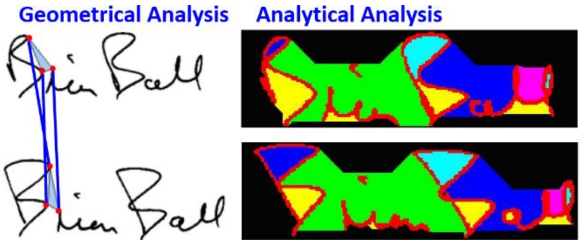
When a majority of voters use VBM because of Covid-19, it becomes apparent that manually comparing signatures is impractical from a time and resource standpoint. As a result, some jurisdictions are relying on scanned Automated Signature Verification (ASV) to provide a first-level authentication check. It is similar to the Post Office envelope address-reading system.[45] When a neural network algorithm flags a mismatch, a worker manually inspects the signature.[46] The voter is contacted with steps to fix the discrepancy, and if there is enough time before the final ballot count is completed, mismatches can be corrected. Otherwise, the ballot is rejected.

Machine learning algorithms pre-train and numerically score thousands of genuine and fake signatures, comparing the envelope signature with the ones on file, all without political influence.[47] Algorithms can adapt to signatures that change over time, and at the appropriate confidence level, declare signatures to match. ASV checks take less than a second making it a valuable VBM tool. There are many signature comparison algorithms, each with strengths and



weaknesses. Our signatures constantly change, with features varying such as cursive versus print, capture pad speed, proportion, spacing, slanted versus straight, and even spelling.[48]

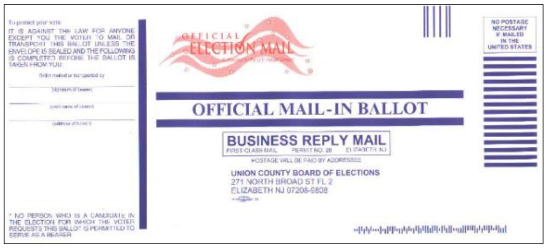
Graphology became a popular handwriting analysis tool in the 19th century and involves the size of letters, angles, slopes, spaces, and more.[49] Geometrical and analytical analysis are two examples of algorithms based on graphology that can help compare signatures. Geometrical verifiers examine the distinctive elements of the signature of record against the envelope signature by building and scoring a comparison of three-node triangles. Similar triangles have a high correlation score and are likely the same signature. Analytical analysis tries to find correlations between signature segments as shown by this color-coded correlation. California officials found no significant increase in ballot rejection using ASV.[50]



Vote Tabulation

On Election Day, votes in all categories of every jurisdiction need to be tallied. In some locations, paper ballots are securely transported to a central site, and in other locations, removable media or printed summaries arrive at town hall for counting. Jurisdictions assemble the tallies from precincts and determine how many votes each candidate or question received.

Absentee and VBM ballots (these can be the same terms in some jurisdictions) have their choices processed by large automated mail sorting machines that identify envelope thickness, weight, and voting precinct to begin VRD tracking.[51]



To protect your vote:
IT IS AGAINST THE LAW FOR ANYONE EXCEPT YOU THE VOTER TO MAIL OR TRANSPORT THIS BALLOT UNLESS THE ENVELOPE IS SEALED AND THE FOLLOWING IS COMPLETED BEFORE THE BALLOT IS TAKEN FROM YOU:

Ballot mailed or transported by

(signature of bearer)

(print name of bearer)

(address of bearer)

* NO PERSON WHO IS A CANDIDATE IN THE ELECTION FOR WHICH THE VOTER REQUESTS THIS BALLOT IS PERMITTED TO SERVE AS A BEARER

OFFICIAL ELECTION MAIL

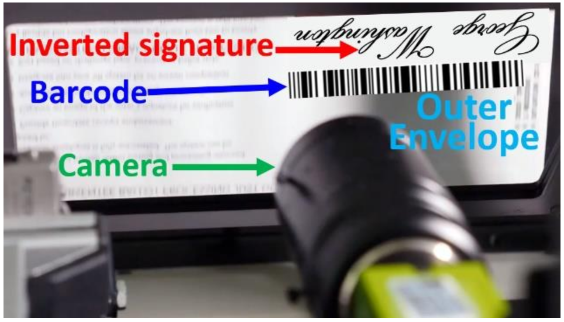
OFFICIAL MAIL-IN BALLOT

BUSINESS REPLY MAIL
FIRST-CLASS MAIL PERMIT NO. 28 ELIZABETH NJ
POSTAGE WILL BE PAID BY ADDRESSEE

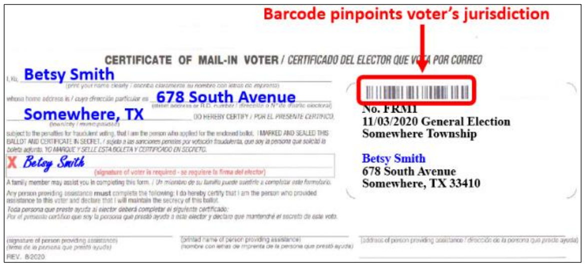
UNION COUNTY BOARD OF ELECTIONS
271 NORTH BROAD ST FL 2
ELIZABETH NJ 07208-9808

NO POSTAGE NECESSARY IF MAILED IN THE UNITED STATES

Based on the jurisdiction, each ballot **outer return envelope** is **barcode** scanned by a **camera** that can process high volumes of **signatures** in a fraction of the time it would take to do manually. In 44 states, **signatures** are validated by machines such as this ES&S Mail Ballot Verifier MBV 1000, which scans and timestamps 100 envelopes per minute, isolating the **signature**. Jurisdictions also use a manual comparison system to display the envelope **signature** and the VRD's set of signatures on a worker's screen.[52,53]



After outer envelope verification, the VRD may be updated with a “ballot processed” timestamp. The envelope then passes through a high-speed opener like this OMATION 410 to the right that slices a fraction of an inch from the envelope’s edge. A worker retrieves an inner envelope, like the one to the left, from the outer envelope.[54] An inner envelope with a voter’s **name**, **address**, and **signature** is scanned. **Betsy Smith’s** VRD entry is updated for a mail-in ballot. At this stage, it is still unknown who she voted for.


Barcode pinpoints voter’s jurisdiction

CERTIFICATE OF MAIL-IN VOTER / *CERTIFICADO DEL ELECTOR QUE VOTA POR CORREO*

I, Yo, Betsy Smith
(print your name clearly / escriba claramente su nombre con letras de imprenta)

whose home address is / cuya dirección particular es 678 South Avenue
(street address or R.D. number / dirección o N° de distrito electoral)

Somewhere, TX DO HEREBY CERTIFY / POR EL PRESENTE CERTIFICO,
(town/city / municipalidad)

subject to the penalties for fraudulent voting, that I am the person who applied for the enclosed ballot. I MARKED AND SEALED THIS BALLOT AND CERTIFICATE IN SECRET. / *sujeto a las sanciones penales por votación fraudulenta, que soy la persona que solicitó la boleta adjunta. YO MARQUE Y SELLE ESTA BOLETA Y CERTIFICADO EN SECRETO.*

X Betsy Smith
(signature of voter is required - se requiere la firma del elector)

A family member may assist you in completing this form. / *Un miembro de su familia puede asistirle a completar este formulario.*

Any person providing assistance **must** complete the following: I do hereby certify that I am the person who provided assistance to this voter and declare that I will maintain the secrecy of this ballot.
Toda persona que preste ayuda al elector deberá completar el siguiente certificado:
Por el presente certifico que soy la persona que prestó ayuda a este elector y declaro que mantendré el secreto de este voto.

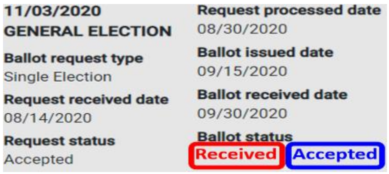
(signature of person providing assistance) (firma de la persona que prestó ayuda)
(printed name of person providing assistance) (nombre con letras de imprenta de la persona que prestó ayuda)
(address of person providing assistance / dirección de la persona que prestó ayuda)

REV. 8/2020

No. FRM1
11/03/2020 General Election
Somewhere Township

Betsy Smith
678 South Avenue
Somewhere, TX 33410

In 36 states, voters have a tracking feedback loop, sometimes through a smartphone app, allowing them to check if their paper ballot was **received** and eventually **accepted**.[55]


11/03/2020 GENERAL ELECTION

Ballot request type
Single Election

Request received date
08/14/2020

Request status
Accepted

Request processed date
08/30/2020

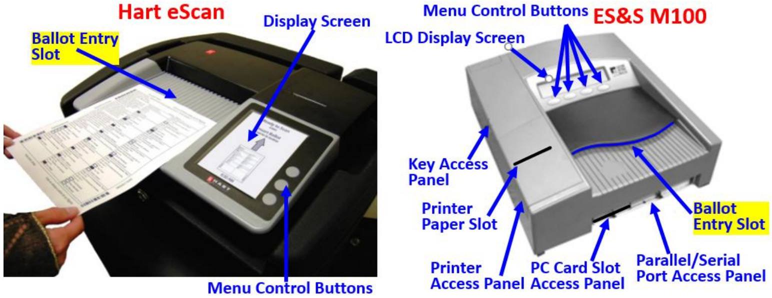
Ballot issued date
09/15/2020

Ballot received date
09/30/2020

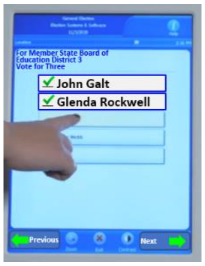
Ballot status
Received Accepted

A machine opens the inner envelope and another worker removes the marked anonymous jurisdiction-specific secret ballot. The ballots are collected, flattened, and sent through an OMR reader. These votes are added to the jurisdiction, county, and state tallies.

Precinct tabulation can occur with ballot scanners such as a Hart Voting Systems eScan or ES&S M100 as shown. The voter slides their finished paper ballot into the **ballot entry slot**. Devices like the M100 run BlackBerry Limited’s QNX, an embedded closed source UNIX-like real-time operating system.[56] Using OMR, both sides of the ballot are simultaneously scanned, and the voter is alerted to under- and over-voted selections. At election close, it prints candidate and question tallies and can transmit encrypted results or store them on a PCMCIA memory card.[57] The scanner retains the ballot in a secure lower compartment as part of its audit trail capabilities.



Advanced DREs like this ES&S DS200 let the voter make choices on a touch-screen without the need for a paper ballot. A barcoded receipt is printed when the votes are cast. The system has a battery backup, proprietary flash drive, audit logs, data encryption, and corruption protection through hash code tabulation.[58] Dominion Voting (former Diebold) and Hart Voting Systems offer similar equipment.


For Member State Board of Education District 3
Vote for Three

✓ John Galt
✓ Glenda Rockwell

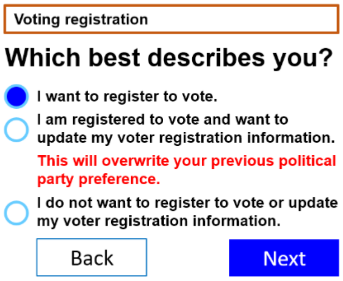
For central processing sites, larger scan and tabulation equipment such as this ES&S DS850 can full image scan 300 ballots per minute and sort them into categories such as counted, write-in choices, and needs manual review (such as when a ballot is not recognized for that precinct.)[59]

After ballots are tallied, the final election is certified and closed. Official notification of those candidates who won and lost their election, as well as any passed or declined referendums or questions is given to officials and the public. Summary totals may be published to a website and released in formats such as comma-separated values and XML.

The Importance of Auditing

Officials strive for fair elections, yet acknowledge that mistakes happen and fraud exists. Perfectly honest people make errors, and machines can be misconfigured, have bugs, or be infected by a computer virus. Administrators rely on independent auditors to ensure election integrity. An audit determines if people and technology performed their tasks correctly, thereby reinforcing confidence that election outcomes are legitimate.

The 2000 Presidential election was a textbook auditing example. Tabulation issues, ballot design, registration, regulations, and operations justified repetitively conducted audits. When election “fraud” is declared, especially as more technology is applied, it makes us doubt the process even more. For example, in 2018, California’s DMV registered new voters through a hacked app like this one that sent the records to Croatia.[60] A VRD log found 100,000 records added to the system, and a software bug added 77,000 duplicate voter records resulting in two registrations for some voters.[61]


Voting registration

Which best describes you?

● I want to register to vote.

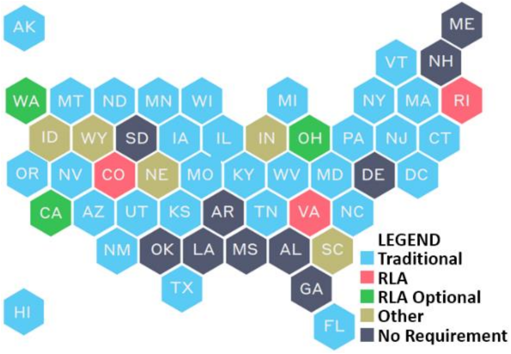
○ I am registered to vote and want to update my voter registration information.
This will overwrite your previous political party preference.

○ I do not want to register to vote or update my voter registration information.

When results are computer recorded and tabulated, it is wise to employ an audit that uses a different process like a paper trail. Paper trails should be voter-verifiable without reliance on a suspect machine. In the U.S., 92% of votes cast have a paper record, and paperless DRE machines are discouraged.[62] The IT world uses the same approach – a storage system backup should be done by a different program and preferably to a medium such as magnetic tape.

An audit should be built into the manual or automated system and be transparent, allowing interested parties to observe accuracy, note issues, and attempt problem resolution. While rare, it may be necessary to repeat an audit, so work products should be kept.

Twenty-two states and Washington, D.C. perform automatic recounts when a small margin of victory is between certain values.[63] There are partial and full recounts, with some limited to a precinct, and others with a statistical Risk-Limiting Audit (RLA) of random ballots to ascertain if there is evidence of a correct outcome. Recounts reinforce election security and resilience by allowing people to inspect ballots. For example, undervoted paper ballots with ovals that were not detected by the scanner, such as this can be corrected, or in the case of the 2020 election, a Floyd County, Georgia election official somehow did not upload votes from a BSD memory card.[64] Audits tend to be unique across jurisdictions and states, just as the voting process tends to be unique. This 2018 "United States" chart shows the lack of audit standardization.[65]



Voter Fraud

Election fraud is probably as old as elections themselves, and a phrase whose meaning changes over time. Historians have reported that George Washington, well before becoming our first president, lost his election to the House of Burgesses at the age of 24 with just 7% of the vote by failing to get voters drunk before the election.[66] The phrase "Swilling the planters with bumbo", meaning supplying the landowners with rum, was a common and clear method of manipulating an election's outcome in 1755.[67]

In the 1860s, William "Boss" Tweed ran a New York City political organization called Tammany Hall.[68] His group was dedicated to having members elected to the NYC government and then use their political power to enrich the Tammany Hall leaders. One method the Boss employed to win an election was to get followers to vote multiple times throughout the borough.

Election fraud is a term that encompasses many aspects of intentional corruption of voting laws and Constitutional amendments, such as the 15th which gave African American men voting rights, and the 19th allowing women to vote. Briefly, **voter fraud** is an illegal behavior such as impersonating another voter to vote twice, selling a vote, a person who votes without the right to do so, the use of a fraudulent address, and others. **Election fraud** is illegal election meddling such as preventing or tampering with voter registration, buying votes, forging candidate petition signatures, tampering with voting machines, illegal acts by officials to exclude qualified voters, altering the tabulation and certification of voting results, and more.

The FBI works closely with all government and private officials to disseminate information, increase security, and stop threats. One of their biggest challenges is to ensure social media, with its different views of reality, is not used by adversaries trying to circulate fake information.[69]

Cybercriminals using the GitHub open source Deepfake algorithm published fake social media videos during the 2020 election to disinform and sway public opinion.[70] Deepfakes (**Deep** Learning & **fake** video) use Artificial Intelligence (AI) autoencoder deep learning algorithms to manipulate videos, making fake events seem real. By encoding images into values and tuning various parameters, a fake image appears similar to the original image. In this example, actor Alec Baldwin's impersonation of President Trump is "enhanced" with a deepfake placing the real President's face on Baldwin.[71] Audio can be manipulated to make the deepfake say things the real person never said.

Actor Alec Baldwin as Donald Trump
Baldwin With President Trump's DeepFake Face

Social media companies like Facebook have policies against fake news. They are creating AI tools that can be 90% effective in spotting false postings, and with deepfakes, they can key in on areas such as eye blink rates.[72] SybilEdge is a trainable Facebook algorithm that finds troll fake accounts that pretend to be friendly and connect with real users (friend requests). Vote trolling starts a quarrel or posts inflammatory comments to decrease trust and sway a vote.[73] Some algorithms detect fake news and prevent clickbait (false content causing a user to click its link). For example, when Donald Trump became the President in 2016, **"*Guess what???? Donald Trump is the Next US President!!!!!!!!!*"** was clickbait for a malicious website.[74]

It can be debated that a confusing ballot design, voter suppression, and asking obtuse ballot questions is an attempt to commit fraud. Examples include insufficient precinct equipment resulting in long lines that dissuade voting, and the Florida butterfly ballot.

Technology can mask fraud and errors. In Pennsylvania, Republican Victor Scomillio earned 54,836 votes in his 2019 race for County Judge while his opponent Abe Kassis had 164.[75] All 100 precincts used certified ExpressVoteXL DRE machines. Election officials were confused when some DREs gave Kassis 0 votes in a system where voters can single-click a party line. Backup paper ballots were checked and showed Kassis beat Scomillio by 1,005 votes, 26,142 to 25,137. What else was wrong? How does the DRE tally show Kassis with 164 while its paper audit trails gave him 26,142 votes? In the same county, a woman voted straight Democrat and all Republican candidates lit up, and a man found his choices would not light up.[76] Could other races with this equipment have incorrect totals and faulty audit trails? Was this a configuration error or hacked equipment? Did the DRE's self-test check the touchscreen's code? ES&S later apologized and said its employees improperly configured the touchscreens and the ballot.

The Pennsylvania incident raises the question – what does voting machine certification mean? According to the U.S. Election Assistance Commission, this optional certification states a system was tested by an approved laboratory and meets VVSG requirements and manufacturer claims.[77] It does not necessarily involve configuration details nor security functionality. Machines are configured long-after testing is complete and security is about preventing an enemy attack. Experience also shows that any large coding effort will have some number of bugs per thousand lines of code, and those bugs could permit or foster unforeseen system behavior.

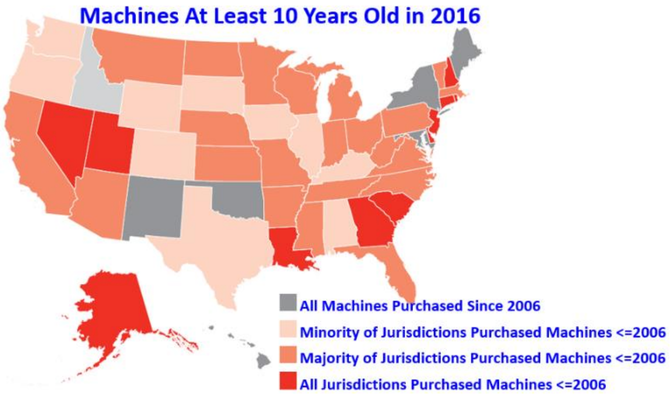
Some elections have the thinnest of winning margins. Any manipulation, whether intentional, accidental, or an act of God can sway an election. For example, on November 7, 2000, in Volusia County, Florida, Al Gore had 83,000 votes to Bush's 62,000. Just 30 minutes later, the Diebold equipment reduced Gore's total by 16,000, with the bulk of the difference going to James Harris, the Socialist Workers Party candidate.[78] The problem was eventually traced to a 600 voter precinct and attributed to either a faulty memory card or a phantom second card.[79]

The Gore – Bush race was very close.[80] Needing 270 electoral votes, the polls closed with Gore at 250 electoral votes to Bush's 246. Gore got to 268 by winning New Mexico by just 355 popular votes (286,783 to 286,417). On November 8, Bush was believed to win Florida by 1,784 popular votes, a margin triggering a recount. By November 10, Bush was ahead by just 327 popular votes. Recounts continued for weeks. Florida's Supreme Court and the U.S. Supreme Court eventually closed the election, with Gore losing and conceding the Presidency to Bush.

Given margins of victory can be small and impacted by fraud, let's examine areas of election fraud from a technology standpoint. In 2017, the Department of Homeland Security (DHS) informed 21 states, including the key electoral vote states of Florida, Ohio, Pennsylvania, Virginia, and Wisconsin, that "bad actors" from Russia targeted their election systems the previous year.[81] While "targeting" is not the same as "broke into", in 2016, hackers using illegally obtained voter registrations for eight states from an election software company sent phishing emails to over a hundred election officials to try to break into their systems.[82] DHS also reported Russia was scanning computers and networks for security holes.[83]

There are many bad actors capable of hacking our systems. What are the vulnerable points of the voting system they could target? Some of the most **susceptible entry points** include the VRD, in-precinct check-in, the voting machines, voter tally, and social media attacks:

Susceptible Area #1 – As we've seen, the registration database is key to generating mail-in ballots and populating precinct DRE voting machines. Election systems are widely reported to be underfunded and often rely on very old equipment, some of which run the registration database.[84] Just like business computers, the concept of "If it ain't broke, don't fix it" seems to prevail. In 2002, the Help America Vote Act injected $2 billion into replacing older machines, but that was almost two decades ago, and in 2016, the Brennan Center For Justice found 43 states still had equipment that was at least 10 years old.[85]


Machines At Least 10 Years Old in 2016
All Machines Purchased Since 2006
Minority of Jurisdictions Purchased Machines <=2006
Majority of Jurisdictions Purchased Machines <=2006
All Jurisdictions Purchased Machines <=2006

In general, when old equipment is linked to a complex network, the entire system can become less secure. A cybercriminal who accesses a system can populate it with fake information and identities, delete records of their choosing, and generate votes for their candidates. As we've seen, in close elections, a difference of a half-percent could be enough to sway an election.

The Washington Post reported Russian agents penetrated the Democratic National Committee's computer network and accessed their database.[86] The 2016 Robert Mueller report to the U.S. Senate titled "Investigation into Russian Interference in the 2016 Presidential Election" documented Russian access to "each voter's name, address, partial social security number, date of birth, and either a driver's license number or state identification number".[87]

Susceptible Area #2 – States use paper and electronic poll books produced and loaded by the VRD to log a voter into the correct polling place, verify their signature, enforce any photo ID requirements, review political party affiliation in the case of a primary, and other functions. EPBs are an example of precinct equipment that needs secure communications with the central location. If a voter cannot check-in, they cannot vote. In 2006, Sequoia Voting Systems EPBs, which is owned by the foreign company Smartmatic, failed voter check-in due to undersized network issues, high transaction rates, and system uptime/reliability.[88,89]

Any networked device, such as an EPB, can be a target for a hacker. Hackers could allow voters and officials to believe a device is correctly recording votes. Even if they do not steal or change user data or otherwise disable the device, they can trigger a denial-of-service attack preventing a precinct from servicing voters. Hackers can also target an equipment manufacturer's proprietary software, perhaps with a virus that spreads to other devices.

Susceptible Area #3 – Voting machines either optically scan paper ballots or are DRE devices that print a paper ballot after prompting the voter to make choices. DREs are manufacturer programmed using non-auditable closed-source code to allow local administrators to use their VMS to configure devices for each precinct's common and unique voting choices. The VMS can leverage USB thumb drives or memory cards which can also contain hacker-provided computer viruses designed to manipulate votes and tallies. VVPT voter receipts and system paper audit trails, produced by many DREs, can help combat the manipulation. They can also help hide a fraud since the paper is printed by the same machine that might have been hacked. A hacked machine could print anything it wants to hide an attack because secret ballots cannot be linked back to a particular voter. Voting equipment manufacturers are secretive about not allowing an independent security evaluation of their machines or the source code running in them.

When the voter signs into a poll book, they are given the next voting number of the day on a paper slip or a DRE voting card. The voter may also be given a blank ballot or directed to an available DRE. The DRE's paper audit trail may be printed sequentially, that is, the first voter on Election Day has their choices printed at the beginning of the audit trail, followed in order until the poll closed. If the audit trail is a sequence of voter's choices, and you were authorized, it is not hard to break the secrecy and determine exactly how a particular voter voted that day.

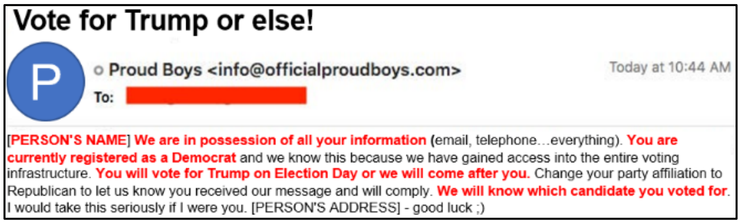
There are dozens of studies looking at hacking DREs, and a Google search reveals pages of hits.[90] Some hacks were documented in the 2006 HBO movie "Hacking Democracy" where candidate Susan Bernecker brought a video camera during her inspection of the DREs stored in a warehouse before Election Day, 1996.[91] She tested the first machine by pressing the button next to her name and her opponents' name, Nick Giambelluca, appears in the vote cast display. She tested 15 machines with identical bad results. Another documentary, "Stealing America: Vote by Vote", is a 2008 examination of election manipulation where not all ballots get counted with claims like "Poll workers watched a hundred and some people go in specifically to that booth and vote. At the end of the day, when that tape came out, one person had voted."[92]

There are also stories about malfunctioning machines, including one that happened to me. A few years ago, I was casting a vote for my son who was running for local office. I voted straight party line and could not get the voting machine to put a **green X** next to his name. I tried multiple times and it would not illuminate. I finally got the voting machine to capture my vote correctly, but apparently, I was not alone. After my son won his election, he told me he got fewer votes than his running mates – that's when I told him what happened to me. Machines can malfunction for a host of reasons including the overuse of hand sanitizer during the pandemic.

Susceptible Area #4 – Vote tallying and reporting is performed by closed-source non-audited systems running on COTS platforms. Until electronic voting systems are auditable, they may be impossible to secure. Similar to **Susceptible Area #3**, a hacker may only need to change a jurisdiction's tally by a few percentage points to have their chosen candidate win an election. Beyond a virus, hackers can delay results through denials of service attacks, install ransomware, and plant social media seeds of doubt into the election's accuracy.

Business computers can be hacked as well as election equipment. Argonne National Labs proved a hacker with just $10 in parts and access to a 2012 Diebold Accuvote TS DRE could alter its functions to change a voter's choices.[93] (NOTE: Diebold sold its election equipment division to ES&S in 2009, which sold it to Dominion Voting Systems in 2010.[94] A portion of the software used in these machines was written in Serbia.[95] Diebold machines are still in use despite their documented problems.[96])

Our hacking insight comes from officials like William Evanina, Director of the U.S. National Counterintelligence and Security Center. He says that foreign adversaries are trying to break into voting systems, spread disinformation, and trying to collect derogatory information about campaigns, candidates, and prominent Americans.[97] "We are very confident that the election infrastructure and posture is very resilient. We are not worried about changing votes at scale. But we are worried about influence on the American voter, and the ability of the American voter to understand where they should get real information, especially when they are voting. How to vote. Where to vote. Be patient when you vote. Be prepared." He said Russia, China, and Iran are using disinformation campaigns, spreading conspiracies and false information to promote candidates they favor and sway the 2020 election. Director of National Intelligence John Ratcliffe said Iran sent threatening allegedly far-right militia group spoofed emails, such as this one, to Florida Republicans using stolen voter data.[98]



Vote for Trump or else!

P

○ Proud Boys <info@officialproudboys.com>

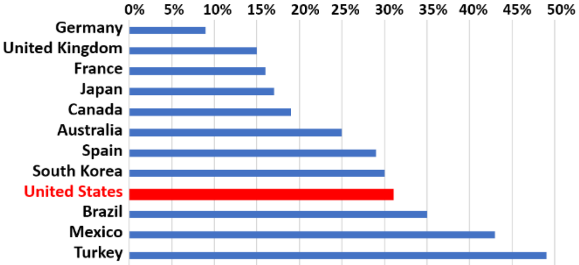
Today at 10:44 AM

To: [redacted]

[**PERSON'S NAME**] **We are in possession of all your information** (email, telephone…everything). **You are currently registered as a Democrat** and we know this because we have gained access into the entire voting infrastructure. **You will vote for Trump on Election Day or we will come after you.** Change your party affiliation to Republican to let us know you received our message and will comply. **We will know which candidate you voted for.** I would take this seriously if I were you. [PERSON'S ADDRESS] - good luck ;)

Voters want to trust election systems, yet in Florida, that trust was broken again. Florida officials had maintained the 2016 election was free from outside attacks. FBI cybersecurity specialists and the DHS, using the Mueller report, secretly informed 67 county election officials in 2019 that Russian hackers used "spear-phishing" attacks targeted at election workers with an email link that downloaded a computer virus.[99] The Russians succeeded at hacking into registration data in at least four Florida counties in 2016, undermining voter trust in Federal officials who kept the information secret for 3 years. Local election officials were blamed for lax security measures.

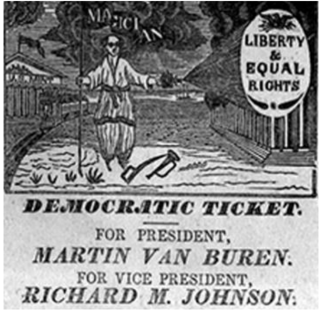
Susceptible Area #5 – Unlike filtered and verified information from reliable newspapers and journalists, some social media sites can knowingly or unknowingly host fake news and AI-inspired open-source programs like Faceswap, allowing almost anyone to post bogus videos designed to spread election fiction, false narratives, and disinform millions of voters.[100] Many sites employ algorithms that keep the reader engaged, and the Reuters Institute shows 1/3 of Americans were exposed to fake news during a week in January/February 2018, stressing election process credibility. The FBI warns that cybercriminals may be trying to create false social media content and websites, which were not specifically engineered to ensure truthful information, to spread disinformation, and undermine elections.[101]



It has become easier for nefarious groups to influence election outcomes by planting doubt and confusing voters through false truths. Companies like Facebook face an uphill battle to fact-check propaganda postings and misinformation. Rather than publish content chronologically, they algorithmically sequence posts and ads based on what they see as relevant to their audience. During the 2020 election, they even scored the journalism through a News Ecosystem Quality algorithm and adjusted the content.[102] More “likes” and clicks mean more ad sales. In 2016, Facebook estimates Russian sponsored ads reached 126 million subscribers.[103]

Future Voting Technology

The history of voting in this country is hundreds of years old, and for the most part, devoid of modern technology. Before the Revolutionary War of 1775-1783, white male landowners not caring about anonymity, and sometimes subject to bribery and intimidation, would yell their votes in public at a carnival or gathering.[104] By the 1800s, voters wrote their names under their candidate’s name or used pre-voted political party ballots as shown here that were stuffed into the ballot box.[105]


LIBERTY
&
EQUAL
RIGHTS

DEMOCRATIC TICKET.

FOR PRESIDENT,

MARTIN VAN BUREN.

FOR VICE PRESIDENT,

RICHARD M. JOHNSON.

Voter privacy became important by 1892 and Grover Cleveland became the first President to be elected by a secret modern paper “Australian” ballot.[106] Sadly, the nature of a secret ballot gave rise to individuals fraudulently voting more than once.

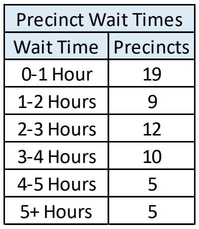
Lever machines in the 1920s tallied voter’s choices with internal mechanical counters, advancing the voting process. In 1962, election technology leaped forward when mark-sense optical scan ballots were introduced. By 1965, voters punched holes in a card next to the candidate’s name, with the cards centrally tabulated. Punched cards were popular until the hanging chad debacle of 2000.[107] The first computerized video voting terminal, controlled by a central computer, appeared in 1974.[108] In 2002, the Federal Election Commission issued Voting System Standards about computer-based election system integrity, the same year Georgia became the first state to use a DRE.[109] The first election Hackathon was held in Las Vegas in 2017 and proved that talented engineers could hack into DREs and VRDs in under two hours.[110]

The goal of future voting technology is to make it easy, secure, auditable, and at a lower cost. Beginning with online voter registration, citizens should be able to register with a smartphone app or in trusted institutions that are open evenings and weekends such as a public library, town hall, or hospital. Citizens could register when starting a new job, through lunch-time office gatherings, or even allow for automatic registration. Using the same security standards as an online loan application, an app could guide us through complexities and instantly check our answers to prevent duplication or conflict when we enter our information. Signatures and photos could be added if available from the DMV or other state agencies, or updated from a military, employee, school ID, or even a selfie. This would result in a more complete and accurate VRD at a lower cost than processing hand-written paper forms.

Voters want to know their choices were secret, which eliminates voter coercion and bribery, and their intentions were properly tallied. We live in a 24/7 connected world, yet general elections tend to be limited to the first Tuesday after a November’s Monday, and election authorities view online voting as inherently dangerous to holding a free and fair election.

To some, losing the ability to observe a citizen voting raises the specter of vote manipulation and interference from others. They yearn for secure, encrypted, verifiable equipment that is hardened to attack and can reproduce vote counts based on voter intentions. Paper ballots, even those generated by BMDs, reflect a century’s old approach to voting and discriminate against voters with disabilities. Paper audit trails are not ideal but currently a good safeguard against fraud. They also look towards systems that are simple to maintain, configure, allow for easier yet reliable registration and data feeds, and help with the accurate VRD purging process.

Voters that deem certain elections as critical are willing to wait in line for early access or Election Day voting. In Maricopa County, Arizona, the average wait in 2020 exceeded two hours. Wait times are basic queuing theory and directly related to voter arrival rates, voter resources, and voting duration.[111] Waiting for



Precinct Wait Times	
Wait Time	Precincts
0-1 Hour	19
1-2 Hours	9
2-3 Hours	12
3-4 Hours	10
4-5 Hours	5
5+ Hours	5

hours can be a challenge, especially during inclement weather. Ways to fix it include:

1. Promote early 7-14-day voting that incorporates weekends.
2. Hold elections on November 11th, Veterans Day. It could be a national work-free holiday.
3. Align work hours so voters can access their precinct during election hours.
4. Allow mail-in voting.
5. Allocate more poll workers and machines to geographic areas based on queuing theory.
6. Add photos to the VRD through DMV registration to speed poll book ID verification.
7. Enable DMV "Real ID" gold star smart chip verification as used by the TSA for airlines.

At the polling place, biometric check-in integrity can be achieved through the same facial recognition system used by the airlines and U.S. customs.[112] In place of a verified photo, fingerprints could be crosschecked against a signature. With state agreement, a Voter ID card equipped with a barcode or embedded chip could be used during registration and voting. [NOTE: The topic of a Voter ID card is hotly debated with claims that seven of the thirty-four states with ID requirements disenfranchise legitimate voters by placing an undue burden on minorities and other groups given the direct and indirect cost to obtain the ID.[113] About 8% of the population, including 25% of eligible African Americans, do not have a government photo ID.[114]]

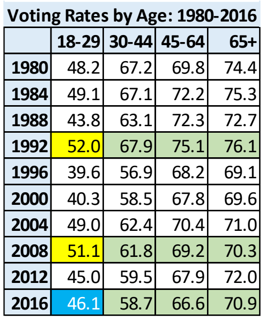
The servers hosting the VDB, processing ballot transactions, and tallying results must use fully verifiable hardware, software, and communications. Multilingual smart apps could use auditable, lower-cost open-source programs that software engineers could examine. An open-source solution would need to establish voter identification, present relevant voter choices, allow the voter to verify their intent, and produce a bank-level ATM-style transaction along with the necessary audit trail. Functionality for disabled, hearing, and visually impaired would be available to these voters through methods they are already familiar with such as Alexa, headphones, or use white letters on a black background in large fonts. The audit ability is a critical element of ensuring a fair election, and today, 92% of votes cast have a paper receipt.[115]

Special hardware, such as a unique touchscreen, should use open-source software and drivers, with checks that binaries are unaltered and virus-free. While this is counter to the current crop of proprietary hardware and software solutions, there is no other easy way to ensure computerized equipment is fraud-free. Open source doesn't guarantee extra scrutiny, but it provides transparency and dissuades malicious code. Reproducible security assessments, test scripts, and scenarios, also part of the public domain, can be used to automatically verify each piece of technology and communication path before, during, and after an election.

It seems inevitable that technology will continue to advance the state-of-the-art approaches to voting. Systems will interface with the mobile culture. It defies logic that you can perform a banking transaction with your Alexa virtual assistant or smartphone but can't cast a vote.

While the goal of election technology is to make voting easier and more secure, modern history shows it can be difficult. The 2020 Iowa Democratic caucus met to select Presidential delegates to the party convention. They used the Shadow company's IowaReporter smartphone app to let 1,700 precincts take a picture of local results and send them to a central office.[116] Unfortunately, a coding error meant the app couldn't handle the volume, leaving many users unable to log in, and those that could found difficulties with the reporting process. The problem caused major delays in caucus results and left citizens feeling the internet was not ready for the elections. It showed that proper testing is needed to gain the public's trust.

While the 2020 election reports showed a greater than 50% voter turnout among young people 18-29, the pattern from recent Census Bureau data shows from 1980-2016, only twice have more than half of young people voted, far less than other age groups.[117,118] It is largely attributable to voting not being an annual habit, apathy, protests, registration time, long lines, transportation, work conflicts, and more. They also found that turnout among those less educated, the poor, and minorities was also lower than the general population. Some expressed their apathy by not voting, or not voting for a Presidential choice.



Voting Rates by Age: 1980-2016

	18-29	30-44	45-64	65+
1980	48.2	67.2	69.8	74.4
1984	49.1	67.1	72.2	75.3
1988	43.8	63.1	72.3	72.7
1992	52.0	67.9	75.1	76.1
1996	39.6	56.9	68.2	69.1
2000	40.3	58.5	67.8	69.6
2004	49.0	62.4	70.4	71.0
2008	51.1	61.8	69.2	70.3
2012	45.0	59.5	67.9	72.0
2016	46.1	58.7	66.6	70.9

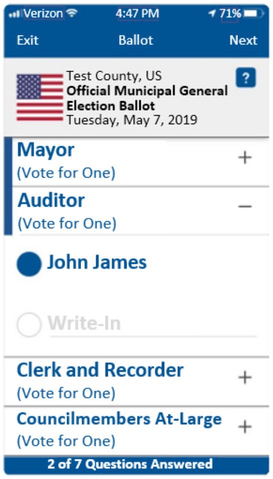
How often have you looked at a live ballot and wondered what a candidate stood for, or if there was a "Consumer Reports"-style scorecard of how well an incumbent kept their past promises? Standing in a voting booth under time constraints is not the time to do candidate research. Many vote a party line because they don't know individual candidates. If they could vote from home on their smartphone or even their smart tv, they could take more time to click for trustworthy and easily understood candidate information before voting. Technology has made everything from banking to shopping easier in recent years – why not voting? Today, technology can provide the "plumbing" to address this need, such as BallotReady, which offers information from nearly twenty categories on any local ballot candidate, such as their views on civil rights, the economy, and healthcare. BallotReady can even help build a ballot of choices.[119]

We would all like to be able to find candidates and propositions that truly represent our interests, however, marrying technology with human nature is difficult. It boils down to politics and biases, leaving little agreement on impartial factual candidate analysis. While the Democrats point to the nonpartisan League of Women Voters (LWV) as a trusted source, the Republicans often say the LWV holds liberal views.[120] Until groups reach a consensus or are aided by AI, technology is limited to present "your side's" view of a candidate's position. And of course, history and candidate background is not a promise of how they will legislate if elected.

New Voting Equipment

Given the history of voting, it is encouraging to see new companies introduce ways to solve election industry issues. Democracy Live is a company whose app, OmniBallot, can use almost any smartphone, tablet, or PC, allowing a voter to fill out a ballot from wherever they are.[121] Designed for the military's need for absentee ballots, it also helps voters with disabilities and those living abroad. Used in over 1,000 jurisdictions, including West Virginia, the process begins by submitting an absentee ballot request form. County officials return a PIN linked to an online ballot. The voter enters personal information and selects their candidates, enters "write-in" choices, and picks "yes/no" propositions. Alerts are issued for overvotes and undervotes. The last step is a printed signature. When done, the ballot is submitted online, emailed, or printed, and tracked via a website.[122] This system is hosted on the FedRAMP-certified AWS cloud.[123]

In Utah and other jurisdictions, absentee voters use the Voatz app.[124] Like Democracy Live, a voter requests an absentee ballot and installs Voatz using biometrics and an ID selfie or driver's license photo scan to display a ballot. After they make their choices, they securely and privately submit the ballot using biometric facial recognition credentials. With end-to-end encryption, Voatz stores information on "multiple, restricted-access, geographically-distributed servers running on blockchain technology".[125] Paper trails and receipts assure the voter their ballot has been processed. Smartphone voting promises to streamline the process, encourage higher voter turnout, and help prevent issues like rainy day hour-long voting lines.



Test County, US
Official Municipal General Election Ballot
Tuesday, May 7, 2019

Mayor +
(Vote for One)

Auditor –
(Vote for One)

● **John James**

○ Write-In

Clerk and Recorder +
(Vote for One)

Councilmembers At-Large +
(Vote for One)

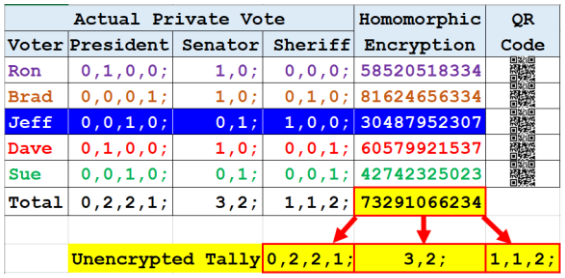
2 of 7 Questions Answered

The Intersection of Cryptography and Mathematics May Hold the Answer

A new approach is being developed by Microsoft's Senior Cryptographer Josh Benaloh to provide total transparency while giving voters confidence their secret choices are secure and counted.[126] His approach uses end-to-end Homomorphic Encryption (HE). In contrast with the 128-bit Advanced Encryption Standard (AES) which requires decrypting an entire string to be usable, HE allows encrypted data to be used or manipulated without ever decrypting it. HE behaves like other public-key encryption methods, but it lends itself to election privacy, patient medical data processing, search engine privacy, and other technology areas.

With a paper ballot or DRE, you verify your vote and submit it for processing. Some may wonder if every vote was counted or might have been altered. Ideally, you also want a receipt for your votes. In this example, **Jeff** uses HE to guarantee his intentions are counted. Using a BMD,

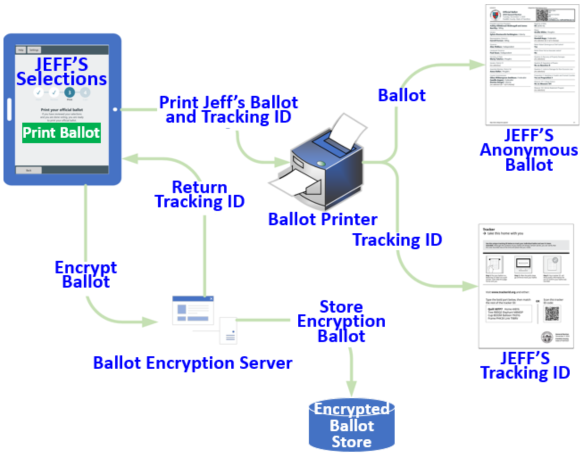
Jeff's receipt has his unique full voting string 30487952307 representing his selection of the 3rd Presidential choice {0,0,1,0}, the 2nd Senatorial choice {0,1}, and the 1st choice for Sheriff {1,0,0}. The receipt includes a URL and QR code to his vote that is stored on a public website that also includes every vote cast by all voters, including those of **Ron**, **Brad**, **Dave**, and **Sue**.[127] To start the tally, the 5 sets of votes are **multiplied** together to form an encrypted tally 73291066234. When 73291066234 is decrypted, we see the 2nd and 3rd Presidential entry each had 2 votes {0,2,2,1}, the 1st Senatorial candidate gets 3 votes {3,2}, and the 3rd Sheriff choice wins with 2 votes {1,1,2}. There was no disclosure or alteration of **Jeff**'s votes, thereby maintaining secrecy. Auditing these results is public and transparent.

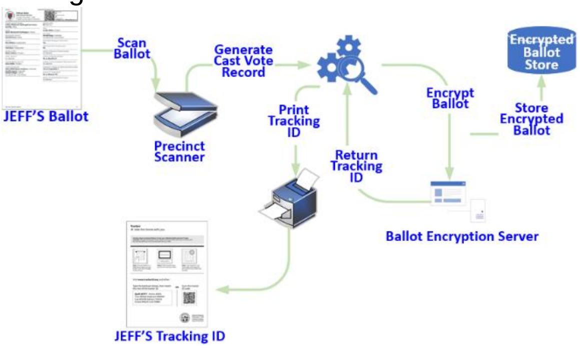


Actual Private Vote				Homomorphic	QR
Voter	President	Senator	Sheriff	Encryption	Code
Ron	0,1,0,0;	1,0;	0,0,0;	58520518334	
Brad	0,0,0,1;	1,0;	0,1,0;	81624656334	
Jeff	0,0,1,0;	0,1;	1,0,0;	30487952307	
Dave	0,1,0,0;	1,0;	0,0,1;	60579921537	
Sue	0,0,1,0;	0,1;	0,0,1;	42742325023	
Total	0,2,2,1;	3,2;	1,1,2;	73291066234	
	Unencrypted Tally		0,2,2,1;	3,2;	1,1,2;

With the URL or QR code, **Jeff** can see his ciphertext votes are intact and counted as intended. Unlike AES, no one learns who **Jeff** or anyone voted for, yet it's all transparent. It is an end-to-end verifiable system allowing groups such as the LWV or the Republican National Committee to quickly reprocess and recount everyone's vote without divulging anyone's name. The system makes it difficult for bad actors to change votes since it is obvious when a vote is altered.

Microsoft incorporated HE into a free, open-source GitHub software development kit called ElectionGuard for use with existing voting equipment.[128] As described, ElectionGuard prints a verification code receipt and a paper ballot for scanning if a BMD was used or directly with a DRE. With finalized election results, all HE codes are publicly published for transparency. To the right is a representation of **Jeff**'s ballot flowing through ElectionGuard once he finalizes his choices and clicks "Print Ballot".[129] To the left, the ballot scanner reads the ballot to cast the vote in the precinct or at the central site. Any party can check if all votes are correctly tallied. ElectionGuard was piloted in Wisconsin in February 2020 and is still in development.[130]





Conclusion

Voting sounds simple. Pose a question, get an answer, and tally the results. Yet history shows it is anything but simple. America's election grid is fragmented, underfunded, complicated, partially staffed by volunteers, occasionally experiences lapses in judgment, burdened by legislative hurdles, partisan, and troubled by annual fraud accusations.

Despite it all, the election system is a work in progress that functions well enough and generally delivers free and fair elections. We have reviewed some aspects of voting irregularities and errors, whether accidental or intentional fraud, and determined that fraud exists and will likely continue. However, fraud is not rampant and generally doesn't radically alter the outcome of elections. The initial review of voter irregularities of the 2020 election cycle concluded it "…was the most secure in American history."[131] Given the state of the art, the only way to have full transparency into vote counts and election certification is the burdensome audit of paper ballots.

Nonetheless, America stands for democracy and the idea of free and fair elections. If just one sentence in the Constitution was amended, election responsibility would fall to the Federal government instead of each state, shrinking the number of permutations and making it easier for technology to reshape.[132] Every jurisdiction interprets "fairness" differently, leaving voting at a crossroads. It was common to wait in line to vote, and with Covid-19, we returned to a society that favors paper ballots and people to deduce if our signature is genuine. Claims of fraud are still with us, with some attacking the Post Office, others accusing foreign agents of interference, and some making suggestions on how to vote twice. It is unlikely we have spotted every case of fraud, but from 2000-2014, there were only 31 impersonation cases out of 1 billion votes cast.[133]

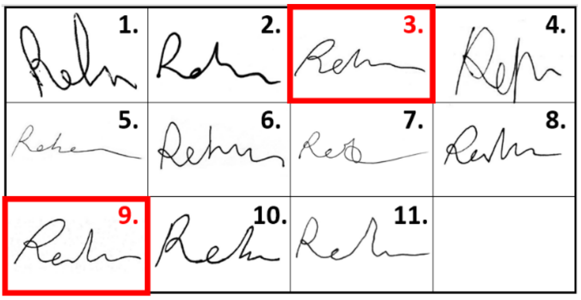
Do we continue the paper ballot trend? Society relies on the internet and smartphone transactions, cloud-based AI home speakers to perform banking transactions, GPS directions, and other disruptive innovations. It seems inevitable that technology, such as homomorphic encryption, will help reshape America's election system. Election modernization should allow us to vote 24/7 weeks before Election Day, provide unbiased insight into choices, and encourage all eligible Americans to vote.[134]

Technology can heal political divisions, unify citizens, and help us select qualified leaders by insisting on credibility, inclusion, transparency, and accuracy in our democratic system. As we become smarter voters, we should hold officials to their oath.

> *"I do solemnly swear that I will faithfully execute the Office of President of the United States, and will to the best of my ability, preserve, protect and defend the Constitution of the United States."*

Forward-thinking democracies inevitably need advanced voting infrastructures. But how precisely and at which degree should they be deployed is complicated. When we think of voting technology, probably what comes to mind is an app or website you could log onto with a very clean interface with all the information you'd need and the ability to vote through that interface.

Earlier in the paper, I asked you to pretend you were an election worker trying to compare envelope signatures against the VRD using a signature matching challenge posted by the NY Times. The answer is number **3** and **9** are the same signature. If you didn't pick the matching signatures, then you would put the corresponding ballot envelope in the mismatched pile and it would require curing.



List of Abbreviations

AES	Advanced Encryption Standard
AI	Artificial Intelligence
ASV	Automated Signature Verification
BMD	Ballot Marking Device
COTS	Commercial-Off-The-Shelf
DHS	Department of Homeland Security
DMV	Department of Motor Vehicle
DRE	Direct-Recording Electronic
EPB	Electronic Poll Book
ETL	Extract, Transform, and Load
HE	Homomorphic Encryption
LWV	League of Women Voters
NCOA	Post Office National Change of Address
OMR	Optical Mark Recognition
QR	Quick Response Code
UI	User Interface
VBM	Vote By Mail
VMS	Voter Management System
VRD	Voter Registration Database
VVPT	Voter-Verifiable Paper Trail
VVSG	Voluntary Voting System Guidelines
XML	Extensible Markup Language

Footnotes

[1] https://worldpopulationreview.com/state-rankings/number-of-registered-voters-by-state
[2] https://worldpopulationreview.com/us-city-rankings/how-many-cities-are-in-the-us
[3] https://sharetngov.tnsosfiles.com/sos/election/minutes/20151201_SECMinutes_VotingMachine.pdf
[4] https://theamericanleader.org/storylines/expansion-of-voting-rights/
[5] https://youtu.be/pI_t66oV6-M
[6] https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8497.1967.tb00802.x
[7] https://learn.cisecurity.org/CIS-Elections-eBook-15-Feb-pdf
[8] “Hart Voting System Support Procedures Training Manual”, https://sos.idaho.gov/elect/Clerk/Hart/ac6300-006_62D_SupportProcedures_%23390-cp.pdf, P. 7
[9] https://www.sos.state.tx.us/elections/forms/sysexam/voting-sys-bycounty.pdf
[10] “Administering Elections: How American Elections Work”, ISBN 978-1-349-55293-1, P. 3
[11] https://constitution.congress.gov/constitution/
[12] https://www.pewresearch.org/fact-tank/2020/11/03/in-past-elections-u-s-trailed-most-developed-countries-in-voter-turnout/
[13] https://www.eac.gov/statewide-voter-registration-systems
[14] https://www.ncsl.org/research/elections-and-campaigns/election-administration-at-state-and-local-levels.aspx
[15] https://ballotpedia.org/Voting_methods_and_equipment_by_state
[16] “Asking the Right Questions About Electronic Voting” by Richard Celeste, Dick Thornburgh, and Herbert Lin ISBN 978-0-309-10024-3
[17] https://news.yahoo.com/mail-votes-could-delay-election-120337599.html
[18] https://www.govinfo.gov/content/pkg/PLAW-107publ252/html/PLAW-107publ252.htm
[19] https://www.acm.org/binaries/content/assets/public-policy/usacm/e-voting/reports-and-white-papers/vrd_report2.pdf
[20] https://ericstates.org/
[21] https://www.elections.ny.gov/NYSBOE/Forms/FOIL_VOTER_LIST_LAYOUT.pdf
[22] https://pages.nist.gov/VoterRecordsInterchange/
[23] https://www.acm.org/binaries/content/assets/public-policy/usacm/e-voting/reports-and-white-papers/vrd_report2.pdf
[24] https://nypost.com/2000/11/10/ironic-twist-daleys-dad-helped-steal-vote-for-jfk/
[25] https://www.dnainfo.com/chicago/20161019/downtown/vote-rigged-elections-history-fraud-stolen-trump/
[26] https://www.washingtonpost.com/news/monkey-cage/wp/2017/08/08/heres-a-voter-fraud-myth-richard-daley-stole-illinois-for-john-kennedy-in-the-1960-election/
[27] https://voter.svrs.nj.gov/registration-check
[28] https://dos.myflorida.com/media/696057/voter-extract-file-layout.pdf
[29] https://dataverse.harvard.edu/file.xhtml?persistentId=doi:10.7910/DVN/42MVDX/MFU99O&version=5.0
[30] https://en.wikipedia.org/wiki/James_Hedges
[31] https://knowink.com/product-catalog/poll-pad/
[32] https://votingsystems.cdn.sos.ca.gov/vendors/knowink/ki-2-5-0-sec.pdf
[33] https://www.ncsl.org/research/elections-and-campaigns/electronic-pollbooks.aspx
[34] https://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/
[35] “Human-Computer Interaction and The User Interface”, P. 7, 2018 Dell EMC Knowledge Sharing Article
[36] https://www.idt.com/us/en/document/atc/newelectronics-capacitivetouchscreens-game-changing-technology-jan2011
[37] https://www.eac.gov/sites/default/files/TestingCertification/2020_02_29_vvsg_2_draft_requirements.pdf
[38] www.barsnstripes.com/docs/retailbarcodes.pdf
[39] http://en.wikipedia.org/wiki/QR_code
[40] https://electionconnect.com/cast-your-vote/
[41] https://www.nytimes.com/interactive/2020/10/07/upshot/mail-voting-ballots-signature-matching.html
[42] https://www.aclufl.org/sites/default/files/aclufl_-_vote_by_mail_-_report.pdf
[43] https://www.newsweek.com/democrats-reliance-easily-disqualified-mail-ballots-could-cost-them-opinion-1538377
[44] https://www.usatoday.com/in-depth/news/investigations/2020/10/08/rejected-mail-ballots-projected-major-factor-2020-election/3576714001/

[45] https://pe.usps.com/businessmail101?ViewName=DeliveryAddress

[46] https://www-cdn.law.stanford.edu/wp-content/uploads/2020/04/SLS_Signature_Verification_Report-5-15-20-FINAL.pdf

[47] https://www.parascript.com/wp-content/uploads/2020/05/SignatureXpert-for-VBM-brochure.pdf

[48] https://www.sos.state.co.us/pubs/elections/docs/SignatureVerificationGuide.pdf

[49] https://www.bbc.com/news/magazine-22198554

[50] https://www-cdn.law.stanford.edu/wp-content/uploads/2020/04/SLS_Signature_Verification_Report-5-15-20-FINAL.pdf

[51] https://www-cdn.law.stanford.edu/wp-content/uploads/2020/04/SLS_Signature_Verification_Report-5-15-20-FINAL.pdf

[52] Connecticut, District of Columbia, Iowa, Maryland, New Mexico, Vermont and Wyoming do not perform signature verification. https://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx

[53] https://www.essvote.com/blog/video/video-mail-ballot-verifier/

[54] https://www.quadient.com/en-AU/mail/document-handling-equipment/omation-306

[55] https://www.realclearpolitics.com/articles/2020/05/06/there_were_not_28_million_missing_mail-in_ballots_143123.html#!

[56] https://en.wikipedia.org/wiki/QNX

[57] https://www.usenix.org/legacy/event/evt08/tech/full_papers/aviv/aviv.pdf

[58] https://www.essvote.com/wp-content/uploads/2020/08/DS200_One-Sheet.pdf

[59] https://www.essvote.com/wp-content/uploads/2020/09/DS850_One-Sheet.pdf

[60] https://www.latimes.com/politics/la-pol-ca-california-motor-voter-problems-investigation-20190409-story.html

[61] https://www.latimes.com/politics/la-pol-ca-motor-voter-registrations-errors-20180524-story.html

[62] https://www.fbi.gov/video-repository/interagency-election-security-psa-100520.mp4/view

[63] https://www.ncsl.org/research/elections-and-campaigns/automatic-recount-thresholds.aspx

[64] https://www.ajc.com/politics/georgia-recount-uncovers-2600-new-votes-in-presidential-race/I75NSPYYGNF43HQZBPYKJWJ5MA/

[65] http://electionlab.mit.edu/sites/default/files/2019-06/Election-Auditing-Key-Issues-Perspectives.pd

[66] https://en.wikipedia.org/wiki/Electoral_history_of_George_Washington

[67] https://www.smithsonianmag.com/arts-culture/swilling-the-planters-with-bumbo-when-booze-bought-elections-102758236/

[68] https://www.fasttrackteaching.com/ffap/Unit_4_Cities/U4_Tammany_Hall_NYC.html

[69] https://www.fbi.gov/video-repository/interagency-election-security-psa-100520.mp4/view

[70] https://github.com/iperov/DeepFaceLab

[71] https://thenextweb.com/artificial-intelligence/2018/02/21/deepfakes-algorithm-nails-donald-trump-in-most-convincing-fake-yet/

[72] https://www.theverge.com/platform/amp/2019/6/27/18715235/deepfake-detection-ai-algorithms-accuracy-will-they-ever-work

[73] https://research.fb.com/blog/2020/04/detecting-fake-accounts-on-social-networks-with-sybiledge/

[74] https://www.sciencedirect.com/science/article/pii/S1877050918318210

[75] https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html

[76] https://www.mcall.com/news/elections/mc-nws-northampton-county-elections-complaints-20191227-rlm547dt7raszogqwxyenu2sh4-story.html

[77] https://www.eac.gov/voting-equipment/frequently-asked-questions

[78] https://www.nytimes.com/2000/11/10/us/2000-campaign-florida-vote-democrats-tell-problems-polls-across-florida.html

[79] https://www.nybooks.com/daily/2018/11/05/voting-machines-what-could-possibly-go-wrong/

[80] https://en.wikipedia.org/wiki/2000_United_States_presidential_election

[81] https://www.nytimes.com/2017/09/22/us/politics/us-tells-21-states-that-hackers-targeted-their-voting-systems.html

[82] https://www.nytimes.com/2017/09/22/us/politics/us-tells-21-states-that-hackers-targeted-their-voting-systems.html

[83] https://www.technologyreview.com/2018/08/15/141028/four-big-targets-in-the-cyber-battle-over-the-us-ballot-box/

[84] https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/07/08/election-experts-warn-of-november-disaster

[85] https://www.brennancenter.org/our-work/research-reports/americas-voting-machines-risk

[86] https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

[87] https://cdn.cnn.com/cnn/2019/images/04/18/mueller-report-searchable.pdf, P. 22

[88] https://www.washingtonpost.com/wp-dyn/content/article/2006/10/30/AR2006103001224.html

[89] https://www.coloradoindependent.com/2006/11/26/poll-worker-sequoia-to-blame-not-user-error/

[90] https://jhalderm.com/pub/papers/diebold-ttbr07.pdf
https://security.cs.georgetown.edu/~msherr/papers/sequoia.pdf
https://people.eecs.berkeley.edu/~daw/papers/sarasota07.pdf

[91] “Hacking Democracy” https://youtu.be/6YldIdkjrqM timestamp 5:36

[92] https://www.stealingamericathemovie.org/index.html

[93] https://www.computerworld.com/article/2511508/argonne-researchers--hack--diebold-e-voting-system.html

[94] https://en.wikipedia.org/wiki/Premier_Election_Solutions

[95] https://en.wikipedia.org/wiki/Dominion_Voting_Systems

[96] https://www.votetexas.gov/mobile/voting/systems/accuvote.htm

[97] “Today Show” October 7, 2020

[98] https://www.wuft.org/news/2020/10/20/fbi-investigating-threatening-emails-sent-to-democrats-in-florida/

[99] https://www.sun-sentinel.com/opinion/editorials/fl-op-edit-russia-hack-florida-elections-secrecy-20191028-xrfjiq4vbvelbfwx7chbtlanki-story.html

[100] https://www.weforum.org/agenda/2020/10/deepfake-democracy-could-modern-elections-fall-prey-to-fiction/

[101] https://www.ic3.gov/Media/Y2020/PSA200928

[102] https://www.nytimes.com/2020/11/24/technology/facebook-election-misinformation.html

[103] https://www.npr.org/2019/04/24/716374421/fact-check-russian-interference-went-far-beyond-facebook-ads-kushner-described

[104] https://time.com/4305508/paper-ballot-history/

[105] https://www.history.com/topics/us-presidents/vote-tech-video

[106] https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-8497.1967.tb00802.x

[107] https://votingmachines.procon.org/historical-timeline/

[108] https://patents.google.com/patent/US3793505A/en

[109] https://votingmachines.procon.org/wp-content/uploads/sites/46/vss2002.pdf

[110] https://fortune.com/2017/07/31/defcon-hackers-us-voting-machines/

[111] https://www.brennancenter.org/sites/default/files/analysis/Long_Voting_Lines_Explained.pdf

[112] https://www.cbp.gov/travel/biometrics/biometric-exit-faqs

[113] https://www.aclu.org/other/oppose-voter-id-legislation-fact-sheet

[114] https://www.coursera.org/lecture/digital-democracy/voter-authentication-q8d1V

[115] https://www.fbi.gov/video-repository/interagency-election-security-psa-100520.mp4/view

[116] https://www.theatlantic.com/technology/archive/2020/02/iowa-caucus-app-tech/606094/

[117] https://www.census.gov/newsroom/blogs/random-samplings/2017/05/voting_in_america.html

[118] https://www.nbcnews.com/politics/2020-election/graphic-battleground-state-turnout-2020-election-n1247337

[119] BallotReady.org

[120] https://www.insidernj.com/inside-league-women-voters-flap-gop/

[121] https://democracylive.com/omniballot-online/

[122] https://www.youtube.com/watch?v=Thqjdb50TGM&feature=youtu.be

[123] https://democracylive.com/wp-content/uploads/2020/04/OmniBallot-Fact-Sheet-Democracy-Live-AWS_3.30.20.pdf

[124] https://voatz.com/how-it-works/

[125] https://voatz.com/security-and-technology/

[126] https://builtin.com/cybersecurity/electionguard-homomorphic-encryption

[127] https://youtu.be/BYRTvoZ3Rho

[128] https://github.com/microsoft/electionguard

[129] https://github.com/microsoft/electionguard/blob/main/docs/guide/Verifiable_Election.md

[130] https://blogs.microsoft.com/on-the-issues/2020/02/17/wisconsin-electionguard-polls/

[131] https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election

[132] https://www.senate.gov/artandhistory/history/common/contested_elections/election_laws.htm

[133] https://www.brennancenter.org/our-work/research-reports/10-voter-fraud-lies-debunked

[134] https://www.fairvote.org/voter_turnout#voter_turnout_101

Dell Technologies believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” DELL TECHNOLOGIES MAKES NO RESPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying and distribution of any Dell Technologies software described in this publication requires an applicable software license.