A Plan to End Election Fraud

Democracy Counts!, Inc.

A California Nonprofit Organization

DRAFT

May 14, 2016

Elevator-pitch argument for doing something about election fraud, summary of evidence for existence of fraud, summary of evidence of impact of fraud, summary of proposed solution, goals and timeline, team qualifications.

Dear Mr./Ms \_\_\_\_\_\_\_\_\_\_\_:

Sample Cover letter (or should this be an introduction, with the cover letter kept apart?)

Our elections underpin citizens’ ability to shape our country through their constitutionally-protected right to vote. Yet this is our least-protected right; recently being declared in court to be less important than the right to keep voting software proprietary and secret to protect the business interests of private companies.

Evidence of fraud exists, particularly in the fraught presidential elections of 2000 and 2004 which handed George W. Bush the White House. His presidency resulted in a 5 trillion-dollar “mistake” to wage war in Iraq, which we will be paying off for a generation.

Democratic elections matter: A fair count of the votes could have prevented George W. Bush from ever holding office. The 2000 election was decided by less than 600 votes in Florida and an estimated 3 million votes for John Kerry went missing from the official count in 2004.

Had a thorough audit been in place in these elections, it would have prevented the “flipping” of the election for George W. Bush. We aim to ensure the will of the voter is reflected in democratic elections going forward.

Technology provides the means to create an immutable, time-stamped record of election auditing information, including an “exit vote” which duplicates the votes cast independently to ensure that the official record matches the intention of the voters. This approach is stronger than the exit polling data that underpins the claim that the 2000 and 2004 elections were stolen and creates an indisputable record that can be brought to court to challenge the officially reported results of an election.

Even if our elections are fair, it is unreasonable to ask voters to trust the officially tabulated results without transparency and genuinely independent verification.

Our team is headed by Daniel Wolf, who, while at Harvard Law School, created one of the first guides for election observers. It was used in the 1984 Nicaragua elections.

It is backed by Devin Luker who specializes in military-grade security in software.

With funding and volunteers, we will create a citizen audit of the California primaries and the 2016 presidential election.

Table of Contents

Introduction

Evidence of fraud

Extent and effects of fraud

Proposed solution

Mechanics of the audit

Historical precedents

Campaign strategy

The Democracy Counts team

Budget

Endorsements

What you can do

Introduction

**Election Fraud is Alive and Flourishing in America.**

It has been taboo for decades to talk about election fraud. Yet it almost certainly exists -- and the spread of insecure electronic voting systems has allowed vote stealing and flipping to be conducted with less risk of exposure than ever, in more elections than ever before. Paperless touchscreen machines are especially suspect: researchers have identified extraordinary correlations between the use of touchscreen machines and unusually large winning margins that always benefit just one candidate or party, while the margins in areas using other types of machines in the same election show normal and irregular margins. The unavoidable conclusion that must be drawn is that these elections are being “flipped”, and that candidates who did not win fair and square are taking office illegitimately.

Does this matter? Yes. Stolen elections destroy accountability to the governed and encourage government policies that are inconsistent with majority wishes. And this stimulates distrust, cynicism and resistance to authority.

*Democracy Counts!*, a nonprofit organization, has developed an election audit system that citizens can use to audit their elections and to expose fraud where it exists. We are planning to deploy it nationwide in this November’s elections.

The audit system is absolutely neutral and impartial. It can be deployed by nonpartisan organizations, electoral authorities, independent observer missions, campaigns of any party, and activists of any persuasion. It uses cutting-edge, highly secure, transparent and verifiable software, and will provide credible and convincing *direct* evidence of voter intentions, allowing reliable comparisons with official results. If official results are significantly discrepant, legal teams can use the evidence immediately to request injunctions and to demand thorough internal investigations of suspect electoral machinery.

The legal effects could be profound. Recent court decisions have held that voting machine companies’ right to maintain the secrecy of proprietary software trumps the public right to verify the reliability and truthfulness of election machinery. If audit evidence casts suspicion on suspect systems’ honesty, courts may order investigations, in turn affecting the outcome of important races. We could see the development of case law that increases the rights of the public to accurate voting systems. This would have the effect of magnifying judicial participation in election oversight and producing both legal and political pressure on local jurisdictions to end, once and for all, the travesty of election fraud.

Evidence of Fraud

one-two pages

Statistical, circumstantial, testimonial; expert testing of vulnerability; “red shift” out of synch with demographic trends, unexplained by gerrymandering

Evidence of fraud is littered throughout the history of elections and typically falls into the following categories:

Voter Impersonation (rare): Impersonating a voter to cast a ballot at the polls.

Vote Buying (relatively rare): Paying a voter to vote a specific way.

Gerrymandering (common): Creating districts that ensure demographics favor one party.

Disenfranchisement (extremely common): Preventing certain groups from voting through ID laws, poll tax, intimidation, purging voter registrations, false information, insufficient polling locations or ballots.

Misrecording of Votes (unknown/common): Through ballot stuffing, direct alteration of ballot counts, or alteration of the machines used to record votes, destruction or invalidation of ballots, producing a false count of the votes cast.

Of these, voter impersonation - the type of fraud prevented by ID laws - is almost nonexistent. Vote buying appears to be limited and is likely to affect the outcome of an election only in small, local races. Gerrymandering of districts is common, creating outcomes in which a party claims more seats in government despite receiving less support from their states. Voter disenfranchisement is by far the most evident and widespread method. The miscounting or misrecording of votes is possibly quite widespread, particularly since the adoption of electronic voting machines and ballot scanners, with statistical anomalies, patterns in cumulative vote shares, and discrepancies in raw exit polling data pointing to widespread manipulation of the vote.

One devoted researcher identified just 31 “credible” cases of voter impersonation in 1 billion ballots cast between 2000 and 2014. In the 2012 election, 1.4 million more democratic votes were cast than republican votes, yet Republicans won a majority - 234 seats to 201 Democratic seats in the House of Representatives - due to manipulated district lines.

When the US administers advice on conducting democratic elections internationally, it states:

‘The motivation to tamper with the official results is so strong in any election that only *independent checks* verifying official results will allow faith in the electoral system and allow citizens to trust the results of an election.’

Via the US Agency of International Development, it recommends the use of parallel vote counts, exit polling and election forensics.  All provide independent verification of official results and the evidence to challenge them.

Yet the United States itself relies on the official counts and internal audits alone, supplying no independent counts to check official tallies of votes.

We have no parallel vote count to catch ballot stuffing or misreporting.  Exit polls are small and conducted as tools for media interpretation of results rather than verification, so the raw data is “adjusted” to match official results once official results are known.  Statistical forensics are not routinely conducted to detect anomalies in the voting data and statistical anomalies identified by independent researchers are routinely tossed out as irrelevant to the certification of official election results.

Extent and effects of fraud

– one to two pages

List of potentially fraudulent office holders and discussion of fraud’s addition to government dysfunction and to destructive policies (Iraq war, budget battles, government shutdown, state gerrymandering, culture battles, etc)

Proposed solution

– one page

Strategy of the audit, including legal, with goals, timeline, overall strategy

**The VeriCount Election Audit System**

The only check against official manipulation of the vote is a truly independent source to verify the election result.  We propose to supply that independent check.

In multiple states, citizen observers have reported officials changing hand-counted tallies in order to match the officially reported machine counts in internal audits of ballots.

Further, internal audits cannot detect certain kinds of election fraud conducted through the reprogramming or hacking of electronic voting machines which alone record the vote in some cases even without without paper printouts available to audit.  Such tampering is not only possible: multiple securities experts have demonstrated that it is easy to do and inexpensive, and can even be done without leaving a trace.

DemocracyCounts! aims to organize and supply the tools for civic movements to audit elections in the United States and abroad.  Independent verification of precinct totals creates trust in the system when they are revealed to be accurate, or exposes errors or fraud when discrepancies are found.

**Two-Part Audit**

*The Poll Watcher’s Audit:*

This type of audit is sometimes called a “parallel vote tabulation” or “quick count” because it provides an independent tally of the official numbers reported by the precincts.

Using the DemocracyCounts! app to record images and data in the timestamped database, poll watcher auditors will document polling officials' data inside the polling place.

Information gathered includes: ballot count at the opening of the poll, a manual count of voters to match the count on the sign-in sheet, ballot count at the end of the day, tallies from counts or tabulations, and closing figures sent to the Secretary of State.

This can reveal errors in figures calculated by a central tabulator or reveal “man-in-the-middle” attacks in which election data is intercepted and changed as it is transmitted to the official election recorder.  This is the type of audit used in Turkey’s ‘Vote and Beyond’ initiative.

Poll watching and parallel vote tabulation replicates official numbers supplied by fallible and potentially manipulated voting and ballot scanning machines: if the machines were hacked, both our results and the official results will be incorrect.

*The “Exit Vote Audit”*

Internationally, large-scale exit *polling* is considered the gold standard for determining voter intent in an election and ensuring the election process accurately counted and recorded their votes.  Exit polls utilize statistical inference based on small samples to estimate the outcome of an election.  They are an internationally-accepted means of detecting fraud.

In 2004, under the George W. Bush administration, the US helped to fund a 20,000-respondent exit poll in the Ukraine during their presidential election that illuminated a 12% discrepancy in the official count.  The results of the exit poll were used to overturn the results under pressure from the US State Department and the international community.

Discrepancies between official results and large-scale exit polls have been used to overturn elections in several other countries as well, including Georgia and Serbia.

Unlike exit *polling*, which selects a sample of voters leaving a polling location, an “exit vote” would attempt to capture 100% of the votes in a given precinct by asking voters to record their vote in our system in order to create an *independent record* of the votes to compare with the official count.  This independent record would then be compared to the official count.

Each voter would receive a request to “verify their vote” in our parallel system as they exit the polling location and asked sign an affidavit with their voter registration information affirming that they are voting the same way in the audit as they did in the election.

The vote would be recorded in a public, immutable database, known as a “blockchain,” where the vote could not be fraudulently changed once recorded.

In order to prevent “ballot stuffing” during the audit itself, the app allows just one vote per voter.  The voter affidavits provide a parallel count of the votes entered in the system to prevent the addition of false votes.  If the information is used in court, the validity of the affidavits can be substantiated through interviews with the voters themselves.

The resulting data will provide evidence of the *minimum number of votes* a candidate received.   If the official ​results for a particular candidate are *lower* than the number of votes cast for the candidate in the “exit vote,” the number of votes under-reported ​will constitute a *suspicious* *discrepancy* worthy of further investigation.

​T​h​e sensitivity of this ​exit-vote audit to detect ​fraud depends on the level of participation by voters for a candidate whose totals are at risk of being reduced, whether by error or because of perfidious activity.  Higher participation levels increase sensitivity.If exit polls are the gold standard for demonstrating voter intent, a high-participation exit-vote constitutes a platinum standard: it provides *direct* evidence of voter intent, both individually and in the aggregate.

***Interaction of the Audit Data Streams​***

The greatest value of the poll-watcher data is the information it provides about the *location of the* *error* in the electoral process*.*

If the poll-watcher data -- which simply reproduces the official data collected inside the polling place -- **matches** the exit-vote data, but the official results **differ from both**, then the alteration must have taken place *after* the polling place tally was reported out to the Secretary of State.

If the poll-watcher data and the official results **match**, but the exit vote audit data are **substantially different**, the source of the discrepancy is hacked machines misreporting the intent of the voter.

If the official results **differ** from both the poll-watcher data *and* the exit vote data, then it is probable that errors were introduced **both** by the voting machines *and* during the transmission from polling place to Secretary of State.

Historical Precedents

In 2013, a movement in Turkey organized 27,000 volunteers to audit the ballot boxes of their national elections, calling themselves ‘Vote and Beyond.’  That year, they cross-checked the vote counts for 97% of Istanbul.

In the years since, they have accumulated 140,000 volunteers and have monitored ballot boxes in five elections, including one presidential election.

This civic movement has increased transparency and trust in the results of the elections.  Where they have verified accuracy in the count, they have put to bed concerns of rigging the election by tampering with the aggregation of votes.

Vote and Beyond proves that citizens can provide independent verification of official tallies for their own elections through training and organization.

Mechanics of the audit

– one-two pages

The apps, the software engine, and the volunteer auditors

The VeriCount election audit system empowers citizens to audit their elections and to expose fraud wherever it occurs. Audit data will enable legal challenges to suspect elections. Conversely, honest elections can be verified, thereby reducing public cynicism.

The system uses trained volunteer auditors, stationed inside and outside of polling places, to continuously record and upload evidence of voter intent. These independent data streams will produce detailed, high-quality direct evidence of the type required for court challenges. In the event that discrepancies between official results and the audit data point to potential fraud, the auditing organizations will be able to immediately and confidently inform government, campaigns and the media of the irregularities, and go into court with the clear and convincing evidence required to enjoin certification of the results pending a full investigation of the official system and its data.

How the audit system works

The audit comprises an open-source software engine that provides secure functions for voting, recording, counting, and end-to-end verification, plus multiple user-facing apps to transmit audit data to the engine. The two most important apps are the Poll Watcher App and the Exit Voting App. The first allows poll watchers to duplicate all the data collected by official poll workers, creating an independent record that will reveal any tampering that occurs after the polls close. The second allows voters, upon departing their polling places, to sign in as before and anonymously re-record their votes. This will provide a parallel vote count to compare against the official results. And in combination with the pollwatcher audit data, it will show whether discrepancies occurred inside the polling place or in the period between the time the polling place reported its tallies and the tally was reported to the public.

If there is no fraud the audit data and official results should line up; discrepancies, however, will provide the legal basis required for courts to order investigations to determine their cause.

All data are stored permanently: Data are uploaded onto a globally distributed database using blockchain technology. All data transmissions are time- and location-stamped and encrypted using NSA-strength “secure hashing algorithms” (SHA-256 and SHA-512). Once recorded, data cannot be deleted or lost because blockchains always add data and never subtract it. The system is transparent: After the polls close and the private keys are released, anyone with the open-source software can decrypt and examine the raw data.

*The days of election fraud are numbered…*

The audit system is absolutely neutral and impartial. It can be deployed by nonpartisan organizations, electoral authorities, independent observer missions, partisan campaigns, and activists of any persuasion. To assure that professional audit standards are adhered to Democracy Counts! will provide training and logistical support to all users.

Campaign Strategy

Organizational capacity building, marketing strategy (phased), alliance building, partner recruitment, auditor recruiting and training, battleground choices, hardware logistics, last-month campaign logistics, election night analysis, public relations strategy, handoff to legal teams, legal and public relations strategies in ensuing court cases, debriefing and preparing for next phase

After the November 2016 elections we will release the VeriCount audit apps to the world and begin spearheading the creation of an International Federation of Election Auditors.

In 2017 Democracy Counts! will begin gearing up to audit the 2018 midterm elections, and after that the 2020 presidential elections, while continuing to support the worldwide dissemination to pro-democracy organizations of the VeriCount audit tools.

Progress

We have prototyped one app and are well along in building the software engine, which is composed of robust and well-understood components that we are lacing together to suit the needs of the audit functions. Before final deployment we will use crowdsourcing to test and validate the final code.

The Democracy Counts Team

– one-two pages

Form of entity, bios of core team, list of slots being recruited for

**About DemocracyCounts!**

DemocracyCounts! is a non-partisan civic organization dedicated to transparent and fair elections in the US and abroad.  We supply citizens with the tools they need to defend their democratic right to vote.

Kellyn Bardeen

Alec Hahn

Matthew Harper? COO

Eric Hillis

Devin Luker

Michael Nelson, Treasurer

Daniel H. Wolf

Budget

2016 campaign, 2017 capacity building, 2018 midterm Congressional campaign, 2019 capacity building, 2020 presidential, Congressional, State campaigns, 2020+ prognostication

What you can do

Join the funding consortium, recruit your friends

Endorse, join our advisory board

Total 4-year campaign Order of Magnitude budget $XXmillions

Total 2016 budget $XX millions

Need $X million right now