

Saving Our Freedom: Renewing U.S. Election Architecture for the 21st Century

Mission Statement: To establish Pittsburgh as the central location in the collaboration of election reform through the development of cyber law, policy, and security

Background:

In light of recent and historical attacks on our election process, many Americans have lost faith not just in political leadership, but in democracy as a whole. A SurveyMonkey Election Tracking poll between October 6 and 8 of 2016, showed that 40% of responders have lost faith in democracy. Reports post-election have shown even further dismay. If we are to believe that democracy is a shining hallmark of our nation, we should recognize that we are in a crisis. The time is now to restore our faith, and we can do this by renewing our election architecture.

Since the turn of the century, we have endured several unpresented and unparalleled tests. Notably, in 2000 during the presidential race between George W. Bush and Al Gore, voting integrity and rights were at the forefront of political discussion. In 2008, intelligence officials reported that the campaigns of John McCain and Barack Obama were both targets of sophisticated cyber espionage attributed to Chinese government officials. Emails and internal documents were compromised, affecting political discussions and relationships. Then, in August 2011, hackers attempted to access accounts related to both the Obama and Romney campaigns. Hackers also shut down Romney's campaign website for several hours, while the National Republican Congressional Committee was also under attack through various forms, such as distributed denial of service attacks and phishing attempts.

Though paper only ballots have been eliminated, the existing electronic voting infrastructure and direct-recording electronic (DRE) voting machines have been shown to be insecure as well. In 2006, the Emmy nominated documentary "Hacking for Democracy" exposed some of issues with the voting machines used in the 2004 election. Specifically, the documentary brought to light the series of scientific tests known as the Hursti Hack, named after Harri Hursti, who successfully demonstrated that votes on a memory card from a Diebold optical scan voting machine could be surreptitiously altered. Moreover, this hack lead to the identification of 16 previously undiscovered vulnerabilities, per the Voting Systems Technology Assessment Advisory Board (VSTAAB) in collaboration with UC Berkley scientists.

Many people do not realize the vulnerabilities of modern computers, let alone many of these outdated voting machines, which are simply computers running obsolete versions of Windows, such as Windows XP and Windows 2000, with proprietary software on top. Several devices have been found to be susceptible to flipping votes due to poor calibration based on age, no hacking required. In fact, in April 2015, the Virginia State Board of Elections decertified thousands of insecure WinVote machines because every single vote could have been modified.

Several legislative measures were taken to try to address the concerns of both electoral identification and election integrity. The Help America Vote Act (HAVA) was passed in 2002 aimed at raising funding, accountability, and standards. Most notably it created reforms to replace obsolete devices and to create the Election Assistance Commission (EAC) to establish uniform practices across the nation. In 2009, President Obama signed into law the Military and Overseas Voter Empowerment Act (MOVE Act) to provide new voting provisions to members of the military and their family who are living abroad. Local to Pennsylvania, a voter ID law was passed, but it was struck down by the Pennsylvania Supreme Court.

Related the concern of voter identification, President Trump, albeit without offering any evidence, stated that millions voted illegally.

Now, in 2017, intelligence officials, policy makers, lawyers and cyber security professionals continue to investigate events related to interference of the 2016 presidential election. A declassified intelligence report states that the hack of the Democratic National Committee resulted in the compromise of emails, chats, and internal research, and that information was leaked with the design to swing the election for one particular party. Moreover, there is evidence of the bankrolling of troll farms for the purpose of disinformation and fake news. These attacks are currently being attributed to hackers connected to top-level Russian officials.

Another pertinent threat to our election infrastructure are attacks on voter registration databases. According to the Brennan Center for Justice at the New York University School of Law, "The voter registration system in much of our country is frayed. One in four eligible citizens is not on the rolls, and one in eight registration records is invalid or has serious errors." Additionally, cyber hacking of these registration databases pose a great threat to the election, since it is a way to remove a citizen's right to vote all together. This is a clear and present threat, as the FBI also reported attempted intrusions of voter databases in over a dozen states, in which 2 were successfully breached, Arizona and Illinois.

It is with just cause, that on January 6, 2017, the Department of Homeland Security (DHS) classified our election infrastructure as a "critical infrastructure subsector," a designation that provides priority benefits and protections similar to 16 other vital sectors such as energy and emergency services. Furthermore, people are growingly concerned about outdated election devices, inefficient and inconsistent registration, the propagation of misinformation, gerrymandering of districts, voter disenfranchisement, and an overall loss of integrity of the election architecture. Every day most Americans use electronic devices with such ease and confidence that we do not think twice about it. We can purchase a cup of coffee on a phone that is more powerful than the devices we use to vote. The time is now to move to a 21st century system of democracy. To do so we must work to educate the electorate, practice a registration system that actively engages all legal citizens, and ensures that our votes are counted securely and accurately.

Goal and Deliverables:

We at the Institute of Cyber Law, Policy and Security seek to provide a premier conference and location in Pittsburgh where the thought leaders and the key aspects of election policy, law, and security are exhaustively addressed in the progression of a modern election architecture.

We will call for white papers of reform advocates, and evaluate, debate, and vet the proposals from the information presented. We aim to have the designs tested within 6-9 months, so that a solution can be implemented in the 2018 elections.

We will provide research that demonstrates an increase in confidence, efficiency, security, and transparency in the election system.

Some Specific Solutions Proposed in the Field:

- Transaction log of all actions on the voting device to create a full audit trail of events, an end-to-end audit, aka "Black Box" of voting
- Voter Verified Paper Audit Trail (VVPAT)
- Ranked Choice Voting (RCV) (Instant Runoff voting)

- Maine adopted this approach for governor, members of Congress and the state legislature
- Automatic voter registration through existing government systems
- Off location backups of voter record databases
- Systems running minimalistic, secure, open and certified source code
- Homomorphic encryption of ballots
- Simulcast reporting of votes on various websites
- An increased and national standard early voting period
- Internet voting
 - Arizona Democratic Primary experimented with Internet voting, saw double turnout.

Audience: Government officials, non-governmental organizations, academic professors and researchers, consultants, system and network engineers

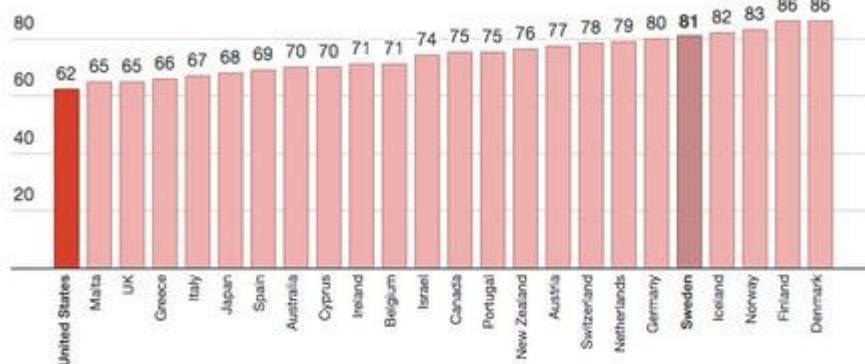
Major Voices in the Field: The Federal Voting Assistance Program, Election Assistance Commission, NIST Accessible Voting Technology, CalTech/MIT Voting Technology Project, Open Source Election Technology Institute, Open Voting Consortium, FairVote, VerifiedVoting.org, Everyone Counts, Common Cause, Electronic Frontier Foundation, VerifiedVoting.org, and VoteTrustUSA, STAR-Vote, The Electoral Integrity Project lead by Harvard Professor Pippa Norris, NYU School of Law's Brennan Center for Justice, and several others.

Conclusion: We believe the time is now to respond with the same fervor and commitment in renewing our right to vote, as those who fought to obtain it. We cannot wait for a "cyber 9/11" to occur as then Homeland Security Secretary Janet Napolitano warned. In a time when we pride ourselves on our technological advancements, let us utilize our cyber resources to create the most engaging, efficient, secure, reliable, comprehensive state of the art election system in the world.

Addendum:

Electoral integrity in 24 Western democracies

Mean PEI index of electoral integrity



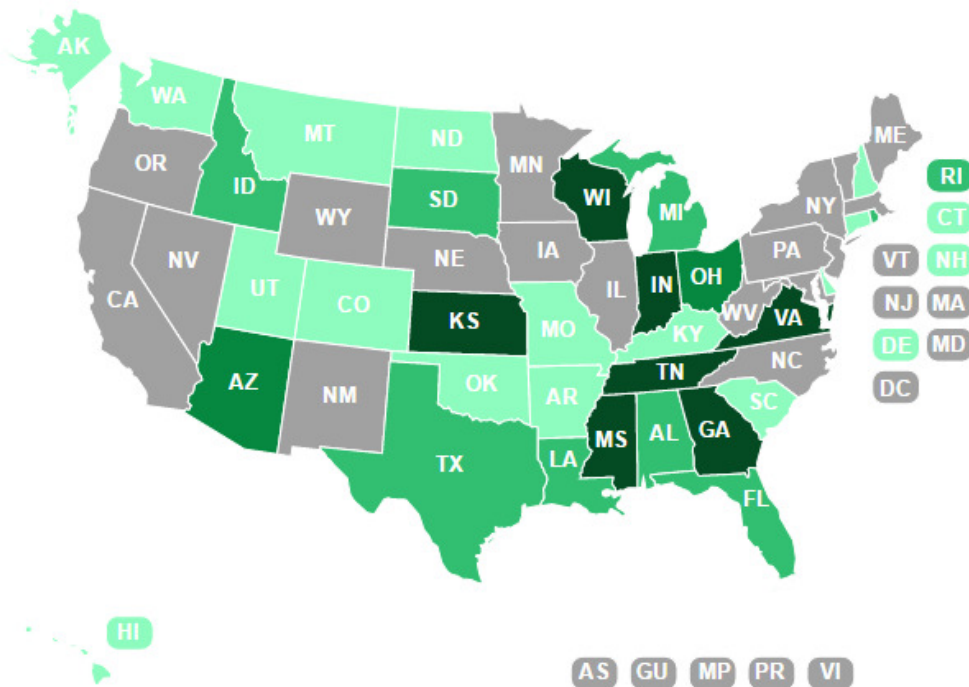
Mean levels of electoral integrity in national parliamentary and presidential elections from mid-2012 to mid-2016.

Source: [The Perceptions of Electoral Integrity expert survey \(PEI-4.5\)](#), Electoral Integrity Project [Get the data](#)

<https://www.hks.harvard.edu/news-events/news/articles/problems-at-the-ballot-box-election-reform-in-the-u.s>

Voter Identification Laws in Effect in 2017

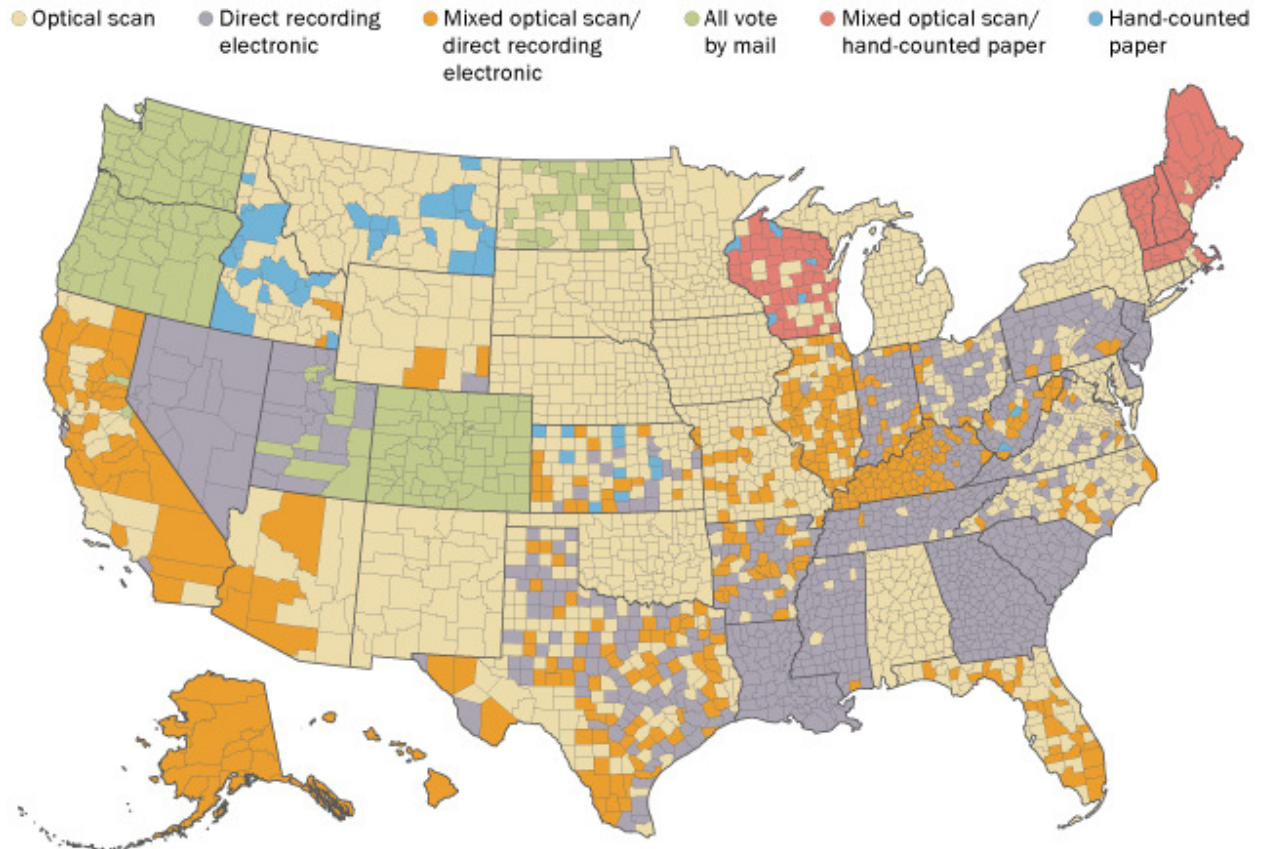
Strict Photo ID	Strict Non-Photo ID	Photo ID requested	ID requested; photo not required	No document required to vote



<http://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx>

Across the U.S., a patchwork of voting methods

Principal voting system, by county



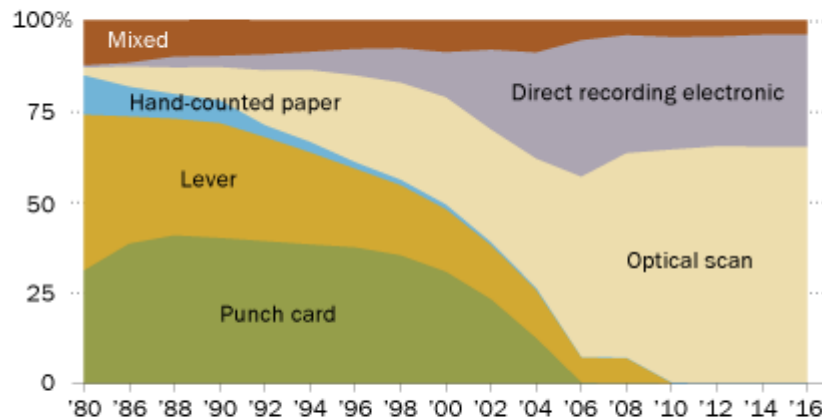
Source: Pew Research Center analysis of data from Verified Voting Foundation.

PEW RESEARCH CENTER

<http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/>

Where did all the punch-card and lever machines go?

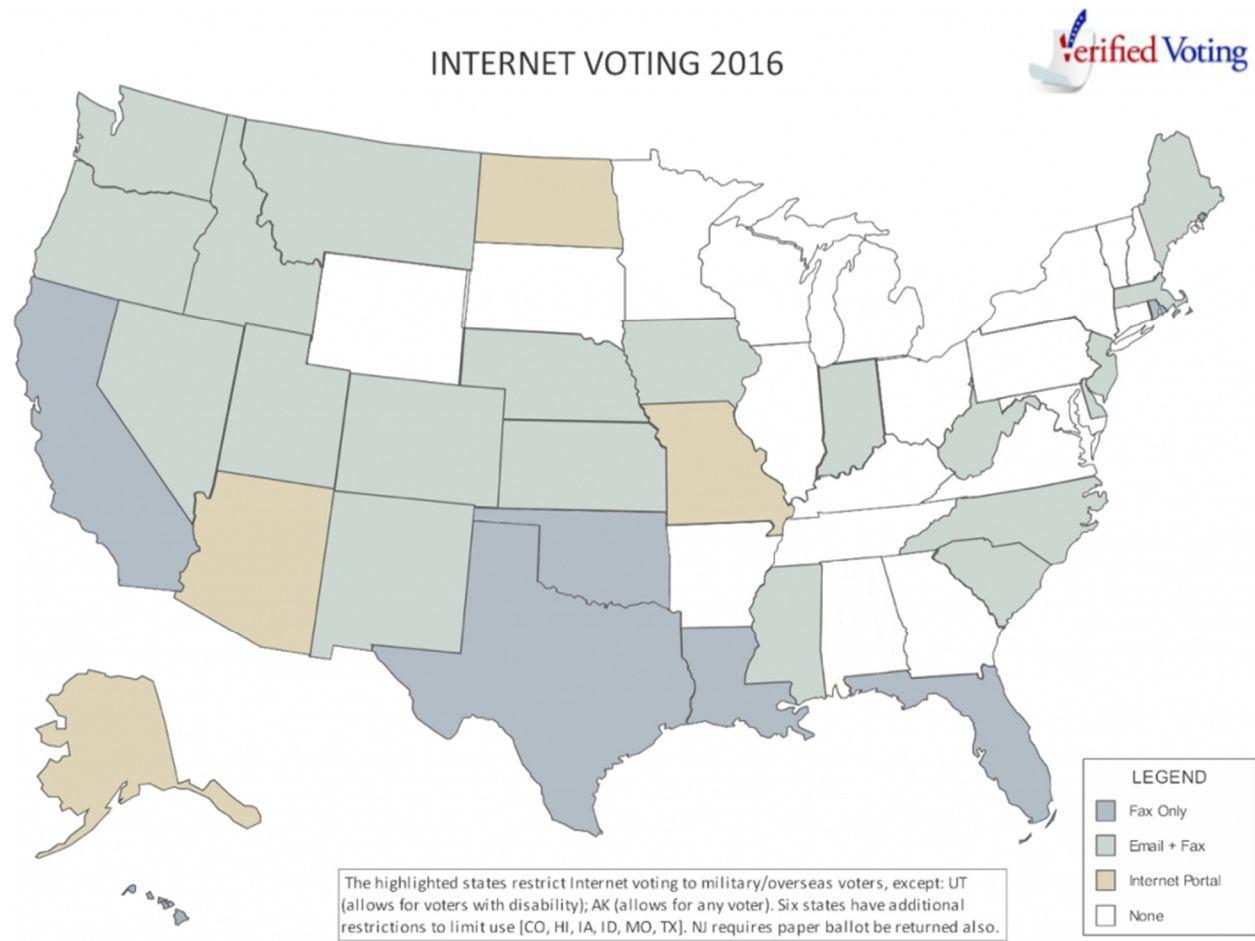
Estimated share of registered voters in precincts using ...



Notes: Excludes precincts that are entirely vote-by-mail. The estimated share of registered voters in precincts using hand-counted paper ballots is 0.1% in 2016.
Source: Election Data Services.

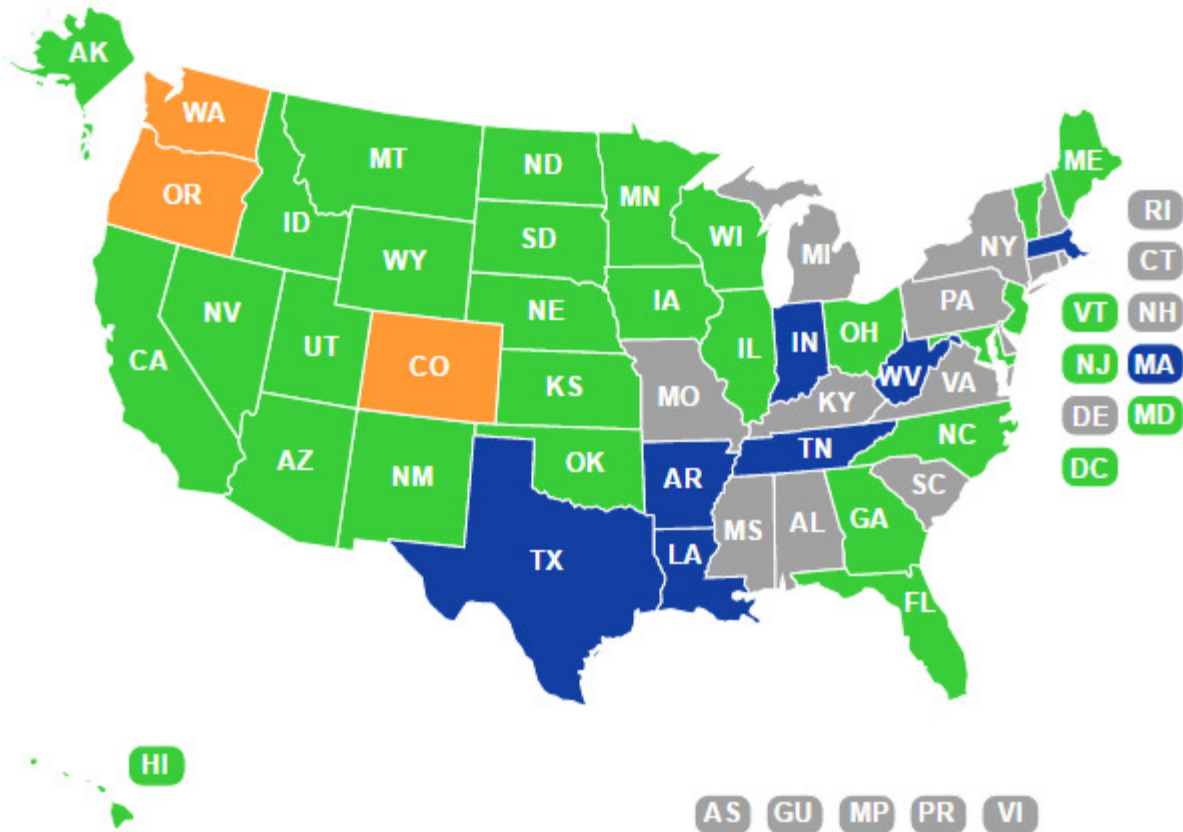
PEW RESEARCH CENTER

“Nearly half of registered voters (47%) live in jurisdictions that use only optical-scan as their standard voting system, and about 28% live in DRE-only jurisdictions, according to a Pew Research Center analysis of data from the [Verified Voting Foundation](http://www.verifyvoting.org/), a nongovernmental organization concerned with the impact of new voting technologies on election integrity. Another 19% of registered voters live in jurisdictions where both optical-scan and DRE systems are in use.” <http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/>



<https://www.verifiedvoting.org/resources/internet-voting/>

No-excuse absentee voting	Early voting	Early voting AND no-excuse absentee voting	All-mail voting	No early voting: excuse required for absentee



<http://www.ncsl.org/research/elections-and-campaigns/absentee-and-early-voting.aspx>