CALTECH/MIT
VOTING TECHNOLOGY PROJECT

A multi-disciplinary, collaborative project of
the California Institute of Technology – Pasadena, California 91125 and
the Massachusetts Institute of Technology – Cambridge, Massachusetts 02139

ELECTORAL VULNERABILITIES IN THE UNITED STATES:

PAST, PRESENT, AND FUTURE

Charles Stewart III, Massachusetts Institute of Technology

Key words: ***American presidential election in 2016***

VTP WORKING PAPER #131

Electoral Vulnerabilities in the United States: Past, Present, and Future

Charles Stewart III
The Massachusetts Institute of Technology
cstewart@mit.edu

A surprising theme of the American presidential election in 2016 was that of election integrity. Despite the fact that election administrators have worked long hours and spent billions of dollars since the disputed presidential election of 2000 to improve elections, and despite a growing body of scholarly work that documents an improvement in election performance since then, the American public was thrown into a panic over the possibility that the 2016 election would be a sham.

Unfortunately, the 2016 election fit a pattern that has been emerging over the past two decades, in which the integrity of election operations themselves have been called into question. In 2016, this pattern was manifest most notably highlighted in charges that Russian interests "hacked" the presidential election, but it also through charges throughout the fall by Donald Trump that Hillary Clinton was "rigging" the election, and through post-election alarm bells rung by Green Party candidate Jill Stein over computerized voting equipment. Even before the general election season had begun, presidential candidates Bernie Sanders and Trump had regularly leveled charges against party insiders that they were stacking the decks against their campaigns in the primaries, through the design of the process and actions taken to advantage other candidates.

The purpose of this paper is to put the issues of election integrity that arose in 2016 in context, and to suggest along the way how it is that one should be sanguine about the administration of elections in the United States. First, I identify four integrity-related themes that have arisen in American elections since the 2000 presidential election. Second, I briefly discuss

what it means to assess the health of the American electoral system, to help confine the scope of this article. Third, I provide two frameworks for assessing the health of the election system, one that takes the perspective of a typical voter, and the other that focuses on the flow of information conveyed in an election. In each of these assessments, I make reference to research conducted over the past two decades that inform our assessment of the health of the election process. I conclude by bringing this discussion back to the specific case of 2016, providing a preliminary assessment of the health of the election process in the most recent federal election.

Four Election-Integrity Themes

Charges of electoral improprieties leveled against political opponents at the national level have been rising over the past two decades, tracing their origins back to the disputed presidential election of 2000. That election, plus the ones immediately following it, established three important themes, or claims, that played out in 2016.

- First, as a general matter, election outcomes can rest on the performance of the voting technology and other aspects of election administration. Because elections are potentially decided by close margins, the choice of a winner can come down to how the election process was conducted, rather than to who legitimately won the most votes.
- Second, America's system of verifying the identity of voters at the polls leaves elections vulnerable to being over-run by ineligible voters (non-citizens, felons), double-voters, and voting impersonators.
- Third, America's reliance on computers to manage elections — all the way from registering voters through casting and counting ballots and reporting the results — leaves the outcome of elections vulnerable to malicious hacking and erroneous computer code.

The first theme, that elections are subject to technological and administrative breakdowns, is a general sentiment that seems to be shared by both the left and the right in contemporary American politics. In fact, it provides the fuel that stokes all other concerns about election administration. The second theme, that non-strict voter identification laws encourage fraudulent voting, tends to be embraced by Republicans and the right more generally.[1] The final theme, that elections are vulnerable to the hacking of voting machines, tends to be supported more often by Democrats and the left.

The 2016 election saw the introduction of a fourth theme, also about computers, but quite different from worries about the hacking of individual voting machines. This is the concern that the computerized infrastructure of elections is vulnerable to attack and disruption. Because of the political context in which this concern was raised in 2016, it probably had greater currency among Democrats; however, because the perpetrators of election-focused cyberattacks in 2016 appear to have been Russian, there is a greater possibility that this fourth (and maybe final) theme will acquire bipartisan ownership.

What Should An Assessment of the Health of the Voting System Focus On?

The swirl of charges relating to election vulnerability in 2016 was at times overwhelming. To assess how well the 2016 election was managed nationwide, it is important, first, to be clear what we are talking about. What is the electoral system we are judging? How do we measure its quality?

The electoral process in the United States, as in any nation, is composed of a variety of distinct systems, each of which complex in its own way, and each of which interact with the others. The public side of the electoral process includes the systems through which candidates

[1] R. Michael Alvarez, Thad E. Hall, Indes Levin, and Charles Stewart III, "Voter Opinion about Election Reform: Do They Support Making Voting More Convenient?" *Election Law Journal* 10(2): 73–87.

are nominated, finance their campaigns, and communicate with voters. This is the part of the electoral process that elicits the most attention from voters and scholars. The electoral process also includes the procedures through which voters and candidates interact with the mechanics of voting, including how candidates qualify for the ballot, how voters register, and how they cast ballots.

This article focuses on this second side of the electoral process, which is often referred to as election administration. This seems appropriate, since the issues raised in the 2000 election — malfunctioning voting machines, inaccurate voter rolls, confusing ballots, etc. — were clearly administrative in nature, as were most of the issues raised in 2016. If we consider the three major electoral-process issues that arose during the 2016 general election — the hacking of the DNC's e-mail servers and charges that Russia was actively intervening on behalf of Donald Trump, charges of millions of illegal voters, and concerns over the accuracy of voting machines — two are clearly in the administrative domain.

Within the field of election administration, scholars have approached the question of system performance from two perspectives. One is a micro-model of the process that focuses on the voter. The other is a macro-model of the process that focuses on the information systems that support elections. I discuss both of them below. Although each approaches the question from a different perspective, they share one important commonality: they each conceptualize election administration as a complex, inter-related system.

Election Vulnerabilities as Seen by the Voter

The Caltech/MIT Voting Technology Project (VTP) suggested one way to frame electoral vulnerabilities in their 2001 report that took a comprehensive look at challenges to election

administration in the United States, *Voting: What Is/What Could Be.*[2] Think of the journey that starts with the voter's decision to vote and ends with the counting of that vote, and imagine the journey flowing along a pipeline, where voters can "leak out" of the system because of system failures along the way. Among these failures are (1) being unable to find the proper polling place, (2) being unable to check-in due to long lines or other polling places problems, (3) encountering a registration problem once at the polling place, (4) encountering an equipment problem, and (5) being victim of a tabulation error.

The 2001 VTP report estimated that in 2000, nearly one million voters in the U.S. had their desire to vote thwarted because of polling place practices such as long lines, between 1.5 and 3.0 million voters were kept from voting because of voter registration problems, and between 1.5 and 2.0 million voters failed to have their vote register because of voting machine failures.[3] It was unable to estimate the number of votes lost due to tabulation errors, nor did it estimate votes lost among voters who relied on the mails to cast ballots.

On this latter issue — lost votes in the "mail channel" of voting — later research suggested that the opportunities for lost votes are even greater than when votes are cast in-person and that the number of lost votes along this channel may rival lost votes that occur on Election Day.[4] The opportunities for lost votes are greater when cast by mail because the process is longer, more complex, and less closely monitored. In traditional absentee voting, for instance, a voter must first request a ballot, which is subject to being lost in the mail or being delayed for administrative reasons; once an absentee ballot is returned to the central voting office, it faces a

---

[2] Caltech/MIT Voting Technology Project, *Voting: What Is/What Could Be*, July 2001. The discussion of this framework follows the discussion in Charles Stewart III, "Losing Votes by Mail," *New York University Journal of Legislation and Public Policy* 13(2010): 573–601, which uses the analogy of a pipeline.

[3] These estimates were derived from studies by the Census Bureau and by analysis of official election statistics reported by the states.

[4] Stewart, "Losing Votes by Mail."

gauntlet of potential challenges — signature verification and vote-counting inaccuracy — that are much more daunting than the analogous procedures in in-person voting.[5]

Figure 1 summarizes this discussion by illustrating the lost-votes pipeline and the major ways in which a voter's intention to cast a ballot can be thwarted through no fault of the voter's own. In the upper portion of the figure, which follows a voter who chooses to vote in-person, we see that the voter must successfully find the polling place (and endure any problems like long lines), have his or her identification validated, and use the equipment. If even one of the following happens — the voter cannot find the polling place, there is a problem with the voter's registration, the voting equipment fails, or there is a tabulation error at the end of the day — the voter's actions are for naught.

[Figure 1 about here]

In the bottom half of the figure, which follows voters who cast a ballot by mail, the voter must request the ballot (often also by mail), the voter's identity must be verified centrally (usually by a signature match) before the ballot can be mailed to the voter, the voter must receive the ballot by mail, mark the ballot, return the ballot successfully, have the voter's identification (yet again) verified centrally, before the ballot is counted. If the original request for the ballot is

[5] According to statistics reported by the U.S. Election Assistance Committee, for instance, in 2012 at least 90,000 mail ballots were rejected at the central office because the signature on the outer "security envelope" either contained no signature or did not match the signature on file with the election office. See U.S. Election Assistance Commission, "2012 Election Administration and Voting Survey," Sept. 2013, Table 33a. (This is a significant under-estimate, because eight states provided no information about why absentee ballots were rejected, and several others provided estimates that were implausibly small.) In some state, voters are allowed to "cure" such problems, but some states do not even notify voters of such problems until after the election. As far as vote-counting accuracy is concerned, the Help America Vote Act (Sec. 301(a)(1)(A)(ii)) requires, for all voters who cast a ballot in-person, that voting systems "provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted," including notifying the voter if she or has has cast a ballot for more than one candidate for a single office. This was to guard against the sorts of problems encountered in Florida in 2000. Voters who are discovered to have over- and under-votes are allowed to correct the situation, if in fact this was due to a voter error. Voters who cast ballots by mail do not have access to such safe-guards. Research suggests that the residual vote rate among absentee voters is greater than the rate among in-person voters, which can easily be attributed to the lack of over- and under-vote protections. R. Michael Alvarez, Dustin Beckett, and Charles Stewart III, "Voting Technology, Vote-by-Mail, and Residual Votes in California, 1990–2010," *Political Research Quarterly* 66(2013): 658–670.

not received, the voter's signature does not match what the central office has on file (either time), the voter is confused by the ballot to the point of over- or under-voting, the marked ballot is lost in the mail, or there is a tabulation error, this voter's actions are also for naught.

Stepping back a bit, the points of failure, or leaks, identified above can be associated with vulnerabilities within the election process that have a wide variety of origins. These origins can be organized into three categories as follows:

- Human error. Election administrators or voters may make honest mistakes in preparing polling places, processing absentee ballots requests, recording who has voted, counting ballots, etc.
- Human malfeasance. Election administrators, voters, candidates, and their supporters may take actions that are intended to thwart the free and fair conduct of the election, such as impersonating a voter, stuffing ballot boxes, or tampering with a cast ballot.
- Administrative practice. An administrative practice may systematically exclude ballots from being counted, such as rules concerning interpreting voter intent.

Consider voting equipment as an example. The "butterfly ballot" episode in Palm Beach County, Florida is a good example of human error resulting in lost votes.[6] In this case, the Supervisor of Elections, Theresa LePore, was responding to a problem caused by the large number of presidential candidates on the Florida ballot (10 candidates, plus a write-in line). If she had simply listed each candidate in the traditional manner, one after the other in a single column on one side of the ballot, she would have had to use a font that was so small, she was worried her voters, who were disproportionately elderly, would be unable to read the names. Thus, LePore adopted a layout that allowed her to alternate the names across two pages, which

[6] Jonathan N. Wand, et al, "The Butterfly Did It: The Aberrant Vote for Buchanan in Palm Beach County, Florida," *American Political Science Review* 95(2001): 793–810.

allowed her to use a much larger font, but which also created confusion about which hole to punch in order to cast a ballot for particular candidates.

Human malfeasance could come in many forms, such as changing the voter's mark on a paper ballot to reflect a different choice, or simply mis-recording tallied vote totals for the purpose of benefitting one candidate over another. Of great concern in some quarters since the early 2000s is the possibility of malicious hacking of computerized voting machines, such as mis-calibrating touch screens so that a selection for Candidate A is recorded as a vote for Candidate B, or "flipping" votes by the vote-counting software.[7]

Finally, administrative error comes into play due to both decisions and practices by election officials that can undermine the accuracy of voting machines. An example of an administrative decision would be a rule that disallows a voter's ballot in a recount because it fails to follow the narrow requirements of the law (such as indicating a vote with an "X" and not a check-mark). An administrative practice might be something like poorly maintaining voting equipment, so that it is more likely to fail. It is likely, for instance, that the problem of "pregnant chad" witnessed in the 2000 Florida recount was due to a build-up of chad from previous elections in the punch card holders; had the holders been cleaned out after every election, as was best administrative practice, the world likely would never have learned the term "pregnant chad."[8]

The 2000 presidential election, which is the source of most recent local, state, and national efforts to reduce the number of lost votes, highlighted administrative and human errors in elections, and drew attention to overcoming them in subsequent reform efforts. For instance,

---

[7] Bev Harris and David Allen, *Black Box Voting: Ballot Tampering in the 21st Century*, Renton, Talion Publishers; Douglas Jones and Barbara Simons, *Broken Ballots: Will Your Vote Count?* Stanford, Center for Language and Information.

[8] Douglas W. Jones, "A Brief Illustrated History of Voting," 2001 (updated 2003), http://homepage.divms.uiowa.edu/~jones/voting/pictures/.

the biggest spending item in the Help America Vote Act (HAVA),[9] a $2 billion appropriation for the purchase of new voting equipment, was intended to allow states and localities to retire older voting machines that were prone to mechanical failure and voter confusion. In addition, HAVA required all states to implement centralized computerized voter registration systems and to implement "provisional balloting" laws, so that voter registration records could be updated more efficiently and that if there was a problem with a voter's registration record on Election Day, the voter would have a "fail-safe" way of voting despite the problem.[10]

Overcoming human malfeasance was not a major theme of HAVA, but in retrospect HAVA's influence on subsequent policymaking targeting malfeasance was significant in two ways, one direct and the other indirect.[11]

The direct influence was the one provision of HAVA that directly addressed potentially criminal behavior — the requirement that any new voter who had registered by mail show some form of identification the first time they voted. This provision was advocated most strongly by Sen. Kip Bond (R-Mo.), whose experience in his home state had convinced him that voter impersonation was rampant, and who blocked passage of HAVA until the voter ID provision had been added to the bill. This, in turn, was the first salvo in what has become an ongoing political war between Republicans and Democratic legislators, at both the state and national levels, over

---

[9] Pub. L. 107-252.

[10] A provisional ballot is used by a voter whose registration is questioned when he presents himself at the voter registration table, and the precinct official is unable to resolve the problem on the spot. Generally, in these circumstances the voter is given a ballot to mark, but the ballot is then placed in a separate sealed envelope (with the voter's identifying information written on the outside of the envelope), with the ballot segregated from the others. After Election Day, the information on the outside of the provisional ballot envelopes is scrutinized by the local elections board, with the voter generally able to bring corroborating evidence about their registration status to the voting office. According to the U.S. Elections Assistance Commission, at least 2.7 million provisional ballots were issued in 2012, of which 2.0 million (at least) were counted, at least partially. Prior to HAVA, if a state did not have a provisional ballot law — and most did not — these voters would simply be sent home, unable to cast a ballot at all.

[11] The following discussion of the legislative history of HAVA and its influence on subsequent election administration politics is adapted from Charles Stewart III, "What Hath HAVA Wrought? Consequences, Intended and Not, of the Post-*Bush v Gore* Reforms," In *Election Administration in the United States: The State of Reform after* Bush v. Gore, *edited by R. Michael Alvarez and Bernard Grofman,* 79–101, New York, Cambridge University Press.

the issue of voter fraud and the need for photo ID.[12] Despite the fact that impersonation fraud is exceedingly rare and that seasoned election lawyers report that voter fraud is commonly the result of "inside jobs" to falsify tabulation reports, to the degree that policymakers and the public have been focused on electoral shenanigans, it has been cast as a problem of voter impersonation.[13]

Second, there was one sleeper detail within HAVA that was regarded at the time as a good-government accommodation for physically disabled voter which, over time, has become a lightning rod for those who worry about computer hackers corrupting the vote count. This provision requires that at least one "direct recording electronic voting system or other voting system equipped for individuals with disabilities" be deployed at every polling place in the United States.[14] Because of the desire of many local administrators to decrease administrative complexity, this accessibility mandate was often implemented by replacing paper ballots (whether hand-counted or scanned) with electronic voting machines.

As local administrators in localities with paper-based systems switched over to electronic systems, a backlash ensued against these new system, which were characterized as being "black boxes,"[15] since most of them stored votes electronically, therefore making it impossible to independently follow the trail from the casting to the counting of the ballot.

This backlash set off a very interesting mobilization effort, spearheaded by computer science professionals, to stop the spread of DREs and, at the very least, require that such

---

[12] Richard L. Hasen, *The Voting Wars: From Florida 2000 to the Next Election Meltdown*, New Haven, Yale University Press, 2012; Daniel R. Bitters and Michael J. Hanmer, "Understanding the Adoption of Voter Identification Laws in the American States," *American Politics Research* (2017), http://journals.sagepub.com/doi/full/10.1177/1532673X16687266.

[13] Lorraine C. Minnite, *The Myth of Voter Fraud*, Ithaca, Cornell University Press, 2010; Mark Braden and Robert Tucker, "Disputed Elections Post *Bush v. Gore*," In *Election Administration in the United States: The State of Reform after* Bush v Gore, New York, Cambridge, 2014, 3–31.

[14] HAVA § 301(a)(3)(B).

[15] Harris and Allen, *Black Box Voting.*

machines have a voter-verifiable paper audit trail (VVPAT) coupled with post-election auditing requirements.

The details of this mobilization are beyond the scope of this article, but one point is relevant here: At the moment of HAVA's passage, virtually none of the active interest groups and policymakers expressed any concerns about the security and administrative vulnerabilities posed by DREs without VVPATs, despite the fact that computer scientists and others had identified vulnerabilities decades before.[16] Over the past decade this activisms has succeeded in rolling back the deployment of DREs.[17] However, the degree of concern over the accuracy of computerized voting systems has not become as widespread and as sharply politicized as the concern over voter fraud and ID, most likely because issues of software vulnerabilities are esoteric to most voters and legislators.

Research conducted since 2000 has suggested that the types of election administration-related problems that were unearthed in 2000 have diminished over time. As early as the 2004 election, the number of votes lost by poorly functioning voting machines dropped by one million compared to 2000, purely as a consequence of voting machine upgrades mandated or facilitated by HAVA. These improvements carried through 2012.[18] Similarly, using the same technique

[16] Roy G. Saltman, "Effective Use of Computing Technology in Vote-tallying: Final Project Report," vol. 75, no. 687 U.S. Department of Commerce, National Bureau of Standards, Institute for Computer Science and Technology, Information Technology Division, 1975; Saltman, "Accuracy, Integrity, and Security in Computerized Vote-Tallying," *Communications of the ACM* 31(1988): 1184–91; Saltman, *The History and Politics of Voting Technology: In Quest of Integrity and Public Confidence*, New York, Springer, 2006.
[17] Charles Stewart III, "Voting Technologies," *Annual Review of Political Science* 14(2011): 353–78.
[18] Charles Stewart III, Residual Vote in the 2004 Election, *Election Law Journal* 5(2006): 158–69; Stewart, "The Performance of Election Machines and the Decline of Residual Votes in the United States," In Barry C. Burden and Charles Stewart III, *The Measure of American Elections*, New York, Cambridge, 2014, 223–47. No research has yet to be conducted that examines the residual vote rate in 2016. One complicating factor for using the residual vote rate to assess the degree of lost votes due to voting technology in 2016 will be the possibility that a measurable number of additional voters abstained in 2016 compared to the immediate past.

utilized in the original Caltech/MIT VTP study, the rate of lost votes due to voter registration problems was estimated to have been cut in half between 2000 and 2008.[19]

In addition, in 2002, the Pew Charitable Trusts first published the Elections Performance Index (EPI), which rates the administrative performance of states in the conduct of elections.[20] The first edition of the EPI covered the 2008 and 2010 elections, and later updates added 2012 and 2014.[21] The EPI was inspired by the work of Heather Gerken, whose book *The Democracy Index*, advocated the use of objective measures of election administration performance to rate states, hoping that low performers on the Index would be prodded to improve.[22] The conceptualization of the EPI borrows heavily from the voter-centric vote of election administration performance first articulated by the VTP in 2001.[23] By the EPI's accounting, election administration, from the perspective of the voter, has improved with each succeeding election.

Electoral Vulnerabilities from an Information Systems Perspective

If the 2000 presidential election highlighted the administrative challenges facing American election administration, the 2016 election highlighted the role of computers in election administration and the vulnerabilities that arise because of the highly integrated nature of the election system. Public awareness of these vulnerabilities came about through three separate news stories that arose during the campaign and immediately after Election Day:

---

[19] Stewart, "What Hath HAVA Wrought?" No follow-up studies on the number of lost votes due to voter registration problems were conducted after 2012, and the data to study 2016 have not been released yet.
[20] Pew Charitable Trusts, "Elections Performance Index," August 9, 2016, http://www.pewtrusts.org/en/multimedia/data-visualizations/2014/elections-performance-index.
[21] A further update for 2016 is in the works.
[22] Heather K. Gerken, *The Democracy Index: Why Our Election System Is Failing and How to Fix It*, Princeton, Princeton University Press, 2009.
[23] Caltech/MIT Voting Technology Process, *Voting*.

- Hacking of the computer systems of the Democratic National Committee, especially its e-mail servers, probably by Russians.[24]
- The targeting of the voter registration systems in twenty states for hacking, including actual infiltrations of these systems in Arizona and Illinois.[25]
- Doubts cast on the accuracy and reliability of computerized vote tabulation equipment.[26] These doubts were expressed most directly by Green Party Candidate Jill Stein, who forced a full recount in Wisconsin and unsuccessfully pursued recounts in Michigan and Pennsylvania.

Unfortunately, these three stories became conflated in the minds of much of the public, so that concern about the actual vulnerabilities to the election administration system was often misplaced. For instance, the hacking of e-mail accounts of the DNC (and possibly the RNC) had nothing to do with election administration, per se, and is best put into the category of old-fashioned political "dirty tricks," albeit with an international cybersecurity flavor. The remaining two stories, about cyberattacks on voter registration systems and the reliability of voter tabulation equipment, are related only because the Internet and vote tabulators rely on electronics and both are used in elections.

To help place these latter two stories about computer-related election vulnerabilities in context, Figure 2 illustrates the information system architecture associated with administering an election.[27] For the sake of discussion, let us call this total system the *election system.* At the

[24] Tom Hamburger and Karen Tumulty, "WikiLeaks Releases Thousands of Documents about Clinton and Internal Deliberations," *Washington Post,* July 22, 2016; David E. Sanger and Eric Schmidt, "Spy Agency Consensus Grows that Russia Hacked D.N.C.," *New York Times,* July 26, 2016.
[25] "U.S. Official: Hackers Targeted Voter Registration Systems of 20 States," *Chicago Tribune*, Sept. 30, 2016.
[26] J. Alex Halderman, "Want to Know if the Election Was Hacked? Look at the Ballots," medium.com, Nov. 23, 2016, https://medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba#.v1f6g27fp.
[27] This figure is a simplified version of a schematic developed by Merle King, Executive Director of the Center for Election Systems at Kennesaw State University. For a full version of the schematic see Merle King, "TGDC

core of the election system is the *voting system*, in which ballots are defined, votes are cast and counted, election counts are displayed, and in which the basic information that might be used to audit (or recount) election results is produced. Embedded in the voting system is the voting machine, but nowadays the voting machine is simply the interface with the voter and poll workers for the capturing and counting of ballots. These other functions — generating ballots and providing auditing information — are also integrated into the voting system.

[Figure 2 about here]

Presently, voting systems in the United States are developed around one of two types of voting machines, one in which votes are captured on paper ballots and then tabulated by scanners, and the other in which votes are captured electronically (similar to an ATM) and then are tabulated by the same machine that captured the vote.[28] For the voting system to work in a computerized environment, a ballot must be defined in software. For a paper ballot, this means laying it out and getting it printed but it also means programming the scanner so that it can interpret marks on the paper. For an electronic ballot, this means laying out the ballot electronically and then loading the ballot imagine into individual voting machines so that touches on the touchscreen can be properly interpreted.

Surrounding the voting system are other systems that support the act of voting. I start with the systems that are "upstream" of the voting system. For in-person voting (early and on Election Day), the voting site will have a poll book of voters eligible to cast a ballot in that location that is consulted when voters present themselves. Some jurisdictions use paper poll

---

Meeting: Scope of Standards and Testing," presentation before the Technical Guidelines Development Committee, National Institute of Standards and Technology, https://www.nist.gov/itl/presentations-tgdc-meeting-feb-8-9-2016. The schematic appears on slide 14.

[28] In 2016, 91.3 million votes were cast on paper systems (71% of all votes), almost all counted by scanners, and 40.1 million were counted on electronic voting machines.

books, which are just paper lists of eligible voters, while others use electronic poll books, which are essentially portable computers with electronic lists of eligible voters.

In turn, the poll books are supported by a voter registration system, which receives voter registration information from a variety of sources and then manages the data for elections. Most new voter registration information comes either from departments of motor vehicles[29] or postcard voter registration forms, although an increasing number of states are now utilizing direct online voter registration portals which interact with the DMV database. The voter registration system is also updated by information that is recorded in poll books used in elections — voter history is updated, for instance, for everyone who turns out, and address changes are often captured when voters present themselves at the polls.

Voters are increasingly voting by mail, and there are systems implemented to track ballot requests and returns. In many ways, the mail ballot delivery/return system can be conceptualized as the mail-ballot analogue to poll books.

Finally, American elections are geographically specific, and entire systems operate to help map (literally and metaphorically) the relationship between voters and the offices for which they are eligible to cast ballots. Some of the information that serves districting systems comes from the voter registration system (such as voter addresses), but additional data must be derived from outside sources, such as geographic information systems (GIS).

Turning our attention to systems down-stream from the voting system, once Election Day is over, tabulated vote results are forwarded to a centralized system that aggregates the results

[29] Under the National Voter Registration Act (Public Law 103-31, *U.S. Statutes at Large* 107(1993): 77–89) eligible registrants must be able to register at a number of state agencies, not just the DMV. Practically speaking, most of these registrants still register through the DMV even though, for instance, they may also interact with state welfare agencies that must also provide voter registration opportunities.

from all voting machines throughout a jurisdiction. Those results are then forwarded on to centralized systems at the state level for further dissemination and aggregation.

The shading in Figure 2 indicates where these component systems are typically located physically. The two systems in the dark gray box — the voting system and poll books — are distributed throughout all the polling places in a local election jurisdiction. Thus, within a single jurisdiction, such as a county, there will be hundreds, and even thousands, of instances of the poll book/voting system interaction displayed in the figure. The light gray box indicates systems that tend to reside centrally within a local jurisdiction. Thus, within a single state, the systems in this area are likely to be distributed in scores of locations.[30] The remaining systems outside this box represent information that comes from or goes outside the control of the local election jurisdiction.

In addition to identifying the principal election systems and their physical locations, Figure 2 describes information flows between the various component systems, with arrows indicating the typical direction of information flow. Some of the information flows are inherently unidimensional, such as when election results are aggregated from the precinct to the jurisdiction and then on to the state, or when the DMV pushes a new voter registration record onto the voter registration system.

Much of the information flow is bi-directional. This is most apparent in the relationships among the voter registration system, poll books, and the mail ballot system. For instance, poll books and mail ballot system serves as a type of customer front-end, capturing address- and name-change information and channeling it to update existing voter registration records. At the same time, the voter registration system provides information to poll books and mail ballot

[30] The one exception here may be the voter registration system, which in some states resides in a central state facility, rather than being distributed among the local jurisdictions.

systems about who is eligible to vote, who has already voted, and which ballot should be given to a voter.

Finally, the arrows in Figure 2 indicate whether, in the typical case, information flows via the Internet[31] (solid lines) or through "air locked" channels, such as thumb drives, smart cards, and even paper (dashed lines). Upstream of the voting system, the voter registration system is the most reliant on the Internet to receive critical information. Even here, most of these connections do not operate in real-time, but rather through the exchange of plain-text files that are updated on a schedule.[32]

Note that all of the information flows for the most critical component system, the voting system, are illustrated with dashed lines. That is because typical practice requires that information moved into and out of these systems be "off the net." For instance, in preparation for an election, a digital scanner must be programmed so that it knows how to read marks on a ballot, and thus tabulate the results properly. Information necessary for this programming is typically loaded into the scanner using a thumb drive or a smart card. On Election Day, voting machines are operated so that they are unconnected to outside computer networks.

An examination of Figure 2 helps to identify which types of vulnerabilities are associated with the different component systems, and in particular, which are more likely to be subject to *widespread* attacks, as opposed to *localized* attacks.[33] Because it is often linked to the outside

---

[31] "Internet" is not strictly the right term to be used here, because some of the computer networks are internal and proprietary.

[32] For instance, voter registration information typically comes from the DVM via a plain-text file that has been deposited in an electronic drop box. That data is then imported into the voter registration system and processed by election officials.

[33] I define a widespread attack as one that is centrally implemented and can be accomplished simultaneously in a geographically distributed fashion. An example of a widespread attack in the non-election world would be a denial of service (DOS) attack intended to disrupt the inventory system of a large online retailer, or a "botnet" that spams millions of e-mail inboxes with virus-laden messages. I define a localized attack as one that targets a specific piece of machinery or a system component in a specific location. An example of this in the non-election world would be

world through multiple Internet pathways, the voter registration system is certainly vulnerable to widespread attacks, whether to commit simple identity theft, maliciously tamper with the information residing in it, or perpetrate a denial of service (DOS) attack. In some cases, the data link between the central voter registration system and local poll books are live in real-time, which could place poll books (but not the voting system) at risk to a widespread attack. Finally, election night reporting systems are similarly vulnerable to widespread attacks, precisely because they function as a portal that interfaces with the general public.

On the other hand, the voting system, including the voting machine itself, is mostly vulnerable to localized attacks. For instance, if a malicious[34] actor wanted to load a corrupted ballot-definition file onto a scanner, she would have to gain access to the computer that creates the ballot definition file to produce the corrupted file, write the file to a physical device like a smart card or thumb drive, walk over to the voting machine, insert the device into the machine, and then load the file into the scanner. Assuming the jurisdiction had multiple scanners, she would need to repeat the process of loading the file into each scanner, one at a time.

Have information system vulnerabilities to the election system grown or shrunk since 2000? Unfortunately, this question has yet to be addressed systematically and objectively, and thus it is not possible to give the same type of comprehensive answer that we can give to the question, "is a voter more or less likely to have her vote lost and uncounted in 2016 than in 2000?" Still, there are hints to an answer to this question. Unfortunately (yet again), it seems that these hints point to the type of "it depends" response that sounds wishy-washy.

---

infecting an individual's desktop computer by accidently booting off of a thumb drive that was infected with a computer virus.

[34] The following also applies to a non-malicious election worker who makes a mistake in the creation of a ballot definition file.

Let us consider the polar ends of the election system, voting system/voting machine end and the voter registration/poll book.

Starting immediately on the heels of HAVA's passage, local jurisdictions began a rush to replace all their machines, paper and non-paper alike, with direct-recording electronic (DRE) equipment.[35] (See Table 1.) The activism discussed above put a brake on this expansion almost immediately, and between 2008 and 2012 the use of DREs began to decline. By 2016, the percentage of voters using DREs had returned roughly to the percentage that had used either DREs or mechanical lever machines in 2000. The fraction of voters using machines with no paper backup is less than is implied by the 29% DRE age in 2016. That is because by 2016, 31% of voters who cast a ballot on a DRE did so on equipment that had paper backups. Thus, the percentage of voters using equipment without paper backups in case of a recount or audit is closer to 21%. As the remaining localities with non-VVPAT DREs replace their equipment in coming years, it is likely that the fraction of voters using completely paperless systems will decline further.

In addition, because of concerns about the accuracy of tabulation systems, the number of states requiring post-election audits has grown. Pew's Elections Performance Index reports, for instance, that 23 states required some form of post-election audit in 2008, growing to 33 by 2014, and to some unknown greater number by 2016.

At the other end of the election information system, opportunities for widespread attacks have grown, as the number of centralized computerized voter registration systems has increased, and as they have become more reliant on the Internet to receive registration information. Reports during the 2016 election that twenty state registration systems showed signs of being probed for

[35] Information about voting technology usage is based on data provided by Kim Brace of Election Data Services. Turnout data is based on data gathered by the author from official sources and acquired from David Leip's Atlas of U.S. Presidential Elections, http://uselectionatlas.org/ (for 2016).

potential infiltrations, and that only two had succumbed, can be interpreted either optimistically or pessimistically, depending on one's perspective. At least one of the penetrations, into the Illinois system, was caused by a SQL injection hack, which is one of the oldest known vulnerabilities of database systems, and is easy to defend against. [36]

Unlike worst-case scenarios involving voting machine hacks, there are back-up options for voters who might find themselves victims of voter registration system hacks. Most notably, provisional ballots were designed precisely for situations in which voter registration problems were discovered on Election Day. Provisional ballots are not perfect, of course, owing to the fact that there is no guarantee that a provisional ballot will be counted, the provisional ballot process can be cumbersome, and the requirement that large numbers of voters cast provisional ballots could easily cause panic among voters. But, at least there are remedies in the law that anticipate such worst-case scenarios, which is not generally true of remedies for widespread voting machine failures, especially those discovered after the polls have closed.[37]

Conclusion, with Some Final Thoughts about 2016

In drawing conclusions about the health of the American electoral system, as evidenced by the 2016 election, the first step is to specify what is, and is not, being included in the analysis. In this article, I have chosen to lay aside some of the most unsavory and disturbing aspects of the

---

[36] Sean Gallagher, "Officials blame 'sophisticated' Russian hackers for voter system attacks," *Ars Technica,*August 30, 2016, https://arstechnica.com/security/2016/08/officials-blame-sophisticated-russian-hackers-for-voter-system-attacks/

[37] Because the legal system places such priority on the finality of elections, courts are very reluctant to order, for instance, the re-running of elections, even when faults have been shown to occur in the running of elections. Justifying the reluctance to order the re-running of elections even in the face of strong evidence of vote fraud was noted in the appellate decision of one of the most notorious voter fraud cases, which involved the 1997 mayoral election in Miami, Florida. The court wrote that "were we to approve a new election as the proper remedy following extensive absentee voting fraud, we would be sending out the message that the worst that would happen in the face of voter fraud would be another election." Se *In re* The Matter of Protest of Election Returns and Absentee Ballots in the Nov. 4, 1997 Election for the City of Miami, Fla., 707 So. 2d 1170, 1171 (Fla. 3d DCA, 1998), *cert. denied,* 725 So. 2d 1108 (Fla. 1998).

election, such as the role of fake news, the manipulation of news due to foreign interference, and the mobilization of intolerance by campaigns and their followers, to focus on the administration of the election itself. This is not because these other factors are irrelevant for drawing larger normative conclusions about how the 2016 election informs our view of the state of democracy in the United States. Rather, it is because the administration of elections is a topic that deserves attention in-and-of itself. After all, the election of 2000 was not beset by fake news, foreign interference, and the mobilization of violence, and yet the poor state of election administration revealed by the Florida recount was alone sufficient to raise larger question about the state of American democracy. Thus, it seems logical to separate evidence about the overall health of the electoral process that arises in the world of the campaign from evidence that arises in the course of administering the election.

Viewed from the perspective of the voter, the election of 2016 was a surprisingly positive experience. Responses to the 2016 Survey of the Performance of American Elections, which was designed specifically with the quality of the voter's experience in mind, reveal few reports of problems on Election Day, and confidence that votes were counted accurately that are on par with the elections of 2008 and 2012.[38] And, despite persistent claims by President Trump that millions of fraudulent votes were cast in the election, diluting the votes of legitimate voters and diminishing his mandate, no more than a handful of potentially plausible cases of illegal voting have been verified.[39]

---

[38] See Presentation of Charles Stewart III to the Pew Charitable Trusts, Voting in America, Dec. 8, 2016, http://www.pewtrusts.org/en/about/events/2016/voting-in-america-2016.

[39] President Trump's insistence that millions of illegal votes were cast in 2016 highlights yet another instance where confusion arises when one does not distinguish between potential threats to election integrity and the success of those threats. To the best we can tell, Trump's charges are based on reports written to estimate the number of people who are registered to vote in multiple states, and the number of dead people who persist on the rolls. See Pew Center on the States, "Inaccurate, costly and inefficient: Evidence that America's voter registration system needs an upgrade," February 2012, http://www.pewtrusts.org/~/media/legacy/uploadedfiles/pcs_assets/2012/pewupgradingvoterregistrationpdf.pdf. In a

Viewed from the perspective of information system integrity, the actual conduct of the 2016 election ended up being anticlimactic.[40] No widespread disruptions of the voter registration system were reported, which of course may have been due in part because of President Barak Obama's call to Russian President Vladimir Putin, telling him to "cut it out."[41] Nor were widespread problems with voter tabulation discovered — underscored by the fact that the statewide recount of Wisconsin paid for by Jill Stein resulted in only a miniscule shifting of election results.[42] And, although it is impossible to prove a negative, the fact that no material news has emerged from the thirty-or-so states with post-election recounts is evidence that any tabulation problems that did emerge were likely localized.

The 2016 election was distinct in the ferocity of the campaign, and in the startling claims made by the winner that the results were marred by voter fraud. It is important to recognize, though, that these were largely differences of degree, not kind, when we consider presidential elections going back to 2000. Sniping by the campaigns over the quality of election

---

nation in which roughly 2% of registered voters move across state lines each year, it is not at all surprising to discover that approximately 3 million individuals would be found on the voting rolls of two states, especially since there is no legal requirement that voters inform their former states of residence that they have moved. The question is not how many people are on the rolls of multiple states, but rather, how many of these vote in the same election in multiple states. Often missing from this controversy is that the Pew report served as a justification for the creation of multi-state compacts precisely to address the problem of multi-state registrations. One of these is the Electronic Registration Information Center (ERIC), which had 20 member-states at the time of the 2016 election, and had already managed to remove one million cross-state movers from the rolls of 13 member states, plus DC, in its first four years of existence. See, http://www.ericstates.org/statistics. The other program is the Interstate Cross-Check Program, which had involved at least thirty states since 2012. The Interstate Cross-Check Program is more focused than ERIC and does not communicate its results as thoroughly as ERIC. Still, the presence of these two programs indicates that to the degree President Trump is basing his charges on hard evidence, it is four years old and does not reflect the efforts undertaken since 2012 to tackle the problem of multi-state registration. On the issue of state efforts to address voter-list accuracy, see National Conference of State Legislatures, "Voter List Accuracy," http://www.ncsl.org/research/elections-and-campaigns/voter-list-accuracy.aspx.

[40] Derek Willis, "Voters encounter problems, but not the ones most feared," *ProPublica Electionland*, Nov. 8, 2016, https://projects.propublica.org/electionland/national/what-didnt-happen/; Jessica Huseman and Scott Klein, "There's no evidence our election was rigged," *ProPublica* Nov. 28, 2016, https://www.propublica.org/article/theres-no-evidence-our-election-was-rigged.

[41] Mark Landler and David E. Sanger, "Obama Defends Muted Response to Russian Hacks" *New York Times*, Dec. 16, 2016, p. A1, https://www.nytimes.com/2016/12/16/us/politics/obama-putin-hacking-news-conference.html.

[42] Wisconsin Election Commission, "Wisconsin recount completed ahead of schedule with relatively small changes to final totals," Dec. 12, 2016, http://elections.wi.gov/node/4768.

administration has become part-and-parcel of every campaign, with positions now hard-wired into partisan predispositions. In this environment, it is important for scholars to be as careful as possible to distinguish between *potential* threats to the health and integrity of election administration and *successful* attacks and failures.

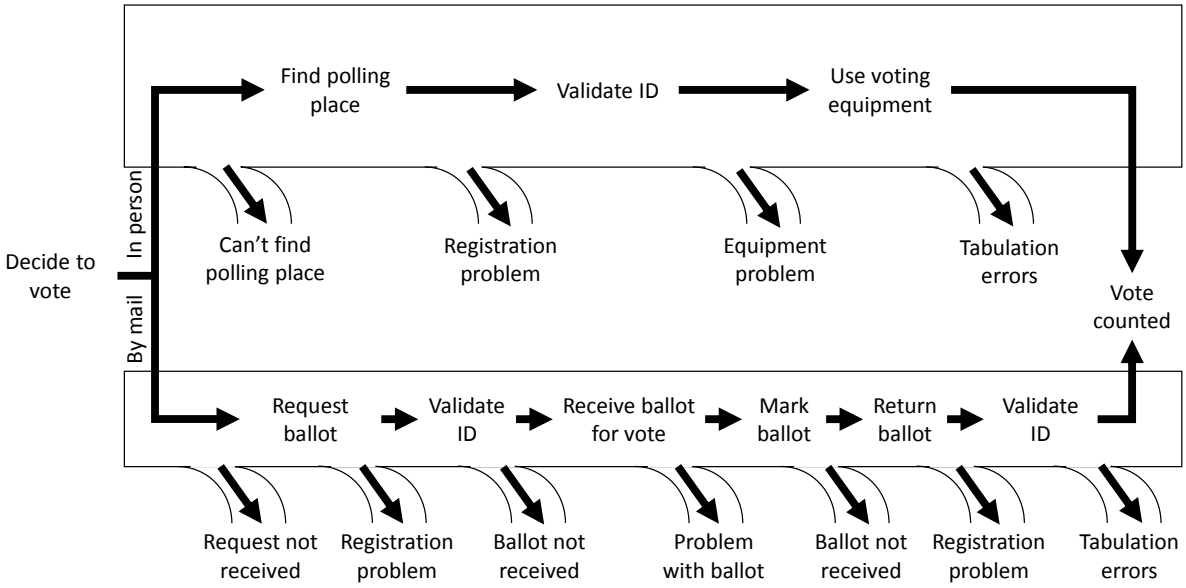
The system is currently set up with ways to guard the health and integrity of the election administration system in the U.S. Efforts made since 2000 to improve administration practice at the state and local level, assisted by federal efforts, are part of that. But, more could certainly be done. Knowing that election administration has become integrated into partisan attitudes and that the sophistication of attacks on the election information system are growing all the time, efforts needs to be expanded to make election administration more transparent and subject to independent verification. Efforts such as the Elections Performance Index can shine a spotlight at a high level on states doing better and worse in this regard. All states should mandate post-election audits of elections, to guard against vulnerabilities of the voting system, and localities that operate paperless voting machines should retire them as soon as possible. Finally, in light of the inherent vulnerability of the voter registration system, states need to find ways to audit the accuracy of their voter rolls and communicate the results (for good or ill) to their voters.

Finally, the source of some of the greatest challenges to the health of the American electoral system is its radically decentralized administration, which draws it roots from federalism. On the one hand, this decentralization becomes an advantage when considering the need to protect against widespread cyberattacks.[43] On the other hand, it disperses expertise and makes it difficult for state and local election officials to organize together against highly

[43] This point was made by FBI director James Comey, when he remarked that the 50-state voting system was so dispersed and "clunky" that it would be difficult for hackers to influence the outcome. Devlin Barrett, "U.S. voting system so 'clunky' it is insulated from hacking, FBI director says," *The Wall Street Journal*, Sept. 8, 2016, http://www.wsj.com/articles/u-s-voting-system-so-clunky-it-is-insulated-from-hacking-fbi-director-says-1473368396.

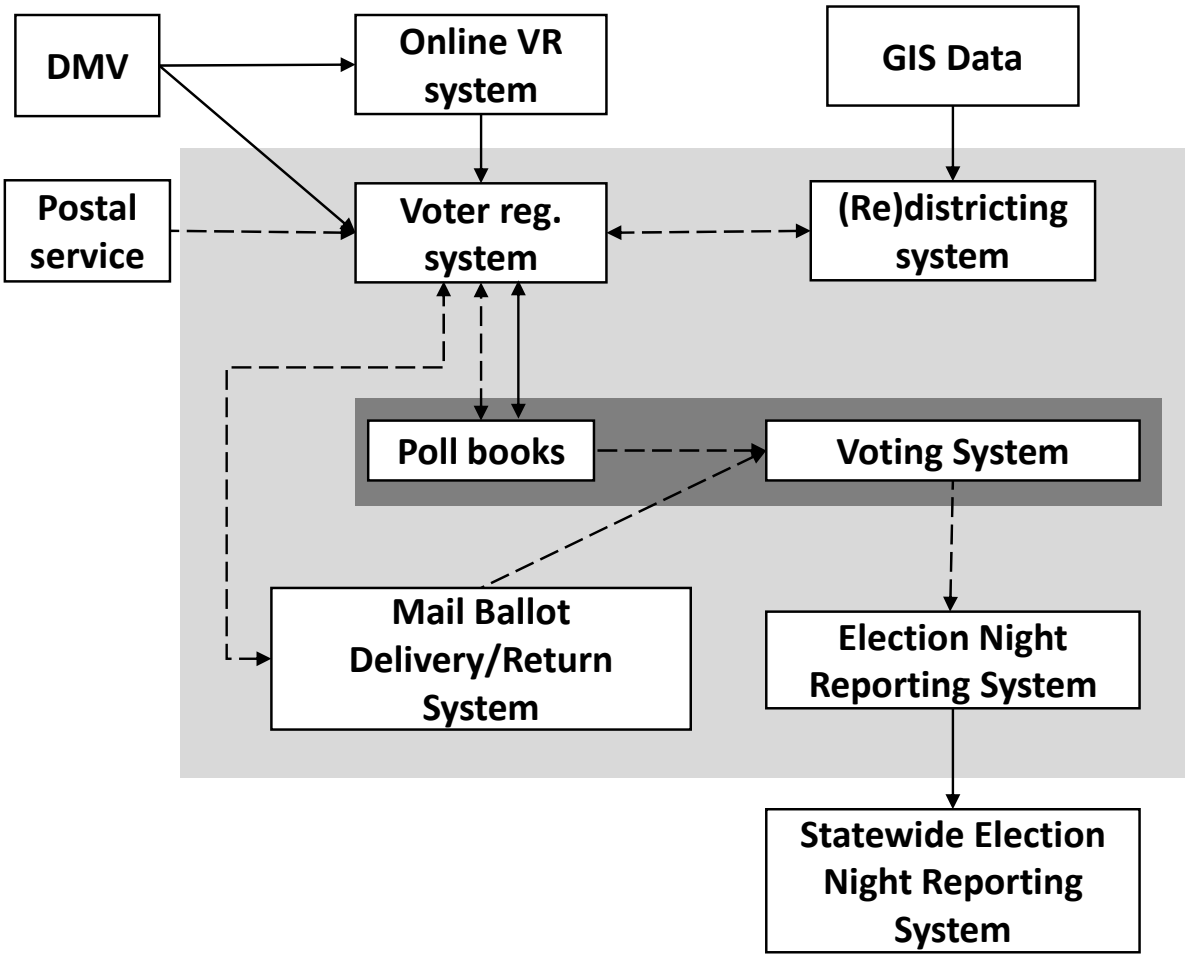
sophisticated cyberattacks that may arise in the future. The question of the federal government's role in ensuring the health and security of the electoral process is certainly one that will gain greater prominence in the years to come.

Figure 1. The voting "pipeline" with opportunities for a voter's desire to vote to be thwarted.



Source: Charles Stewart III, "Losing Votes by Mail," *New York University Journal of Legislation and Public Policy* 13(2010): 573–601,

Figure 2. A schematic view of the election system.



Note: Arrows depict the direction of information flow between component systems. Solid lines indicate flows that typically rely on the Internet or other networks that are connected to the Internet; dashed lines indicate information flows that typically are “air gapped” from outside networks. The dark box indicates systems that are typically deployed in individual polling places; the light gray box indicates systems that are typically centralized in a local jurisdictions’s election office.

Table 1. Use of voting technologies in the United States, 2000–2016.

a. Millions of voters

	2000	2004	2008	2012	2016
Non-paper	**28.6**	**49.0**	**47.4**	**38.9**	**40.1**
Mech. lever machines	17.4	14.8	7.6	0	0
Direct recording electronic	11.2	34.1	39.8	38.9	40.1
Paper	**66.9**	**61.1**	**77.1**	**83.9**	**91.3**
Punch card	35.4	14.7	0.2	0.1	0
Hand-counted	1.6	0.9	0.2	0.2	0.2
Scanned	29.9	45.5	76.7	83.7	91.1
Mixed	**9.6**	**11.7**	**6.8**	**5.8**	**5.2**
Total	**105.1**	**121.8**	**131.2**	**128.5**	**136.6**

b. Percentage of voters

	2000	2004	2008	2012	2016
Non-paper	**27%**	**40%**	**36%**	**30%**	**29%**
Mech. lever machines	17%	12%	6%	0%	0%
Direct recording electronic	11%	28%	30%	30%	29%
Paper	**64%**	**50%**	**59%**	**65%**	**67%**
Punch card	34%	12%	0%	0%	0%
Hand-counted	1%	1%	0%	0%	0%
Scanned	28%	37%	58%	65%	67%
Mixed	**9%**	**10%**	**5%**	**4%**	**4%**
Total	**100%**	**100%**	**100%**	**100%**	**100%**

Note: Column sums are subject to rounding error. "Mixed" counties are those with more than one type of technology. In almost all cases, these are counties that have a combination of hand-counted and scanned paper.

Source: Election technology was supplied by Kimball Brace, Election Data Services. Election returns were collected by the author (2000–2012) and supplied by David Leip, David Leip's Atlas of U.S. Presidential Elections, uselectionatlas.org.