BRENNAN CENTER FOR JUSTICE

VOTING SYSTEM FAILURES: A DATABASE SOLUTION

Lawrence Norden

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at New York University School of Law is a non-partisan public policy and law institute that focuses on fundamental issues of democracy and justice. Our work ranges from voting rights to campaign finance reform, from racial justice in criminal law to presidential power in the fight against terrorism. A singular institution – part think tank, part public interest law firm, part advocacy group – the Brennan Center combines scholarship, legislative and legal advocacy, and communication to win meaningful, measurable change in the public sector.

ABOUT THE BRENNAN CENTER'S VOTING RIGHTS AND ELECTIONS PROJECT

The Brennan Center promotes policies that protect rights, equal electoral access, and increased political participation on the national, state and local levels. The Voting Rights and Elections Project works to expend the franchise, to make it as simple as possible for every eligible American to vote, and to ensure that every vote cast is accurately recorded and counted. The Center's staff provides top-flight legal and policy assistance on a broad range of election administration issues, including voter registration systems, voting technology, voter identification, statewide voter registration list maintenance, and provisional ballots.

The Help America Vote Act in 2002 required states to replace antiquated voting machines with new electronic voting systems, but jurisdictions had little guidance on how to evaluate new voting technology. The Center convened four panels of experts, who conducted the first comprehensive analyses of electronic voting systems. The research proceeded over a period of nearly two years and culminated in two path-breaking reports: *The Machinery of Democracy: Protecting Elections in an Electronic World*, which focused on voting system security, and *The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost*. In the years since the Brennan Center published these two reports, the Brennan Center has helped election officials and jurisdictions ensure that their electronic voting systems are as secure and reliable as possible.

ABOUT THE AUTHOR

Lawrence Norden is Senior Counsel in the Brennan Center's Democracy Program and director of the Brennan Center's Voting Technology Project. He has authored several nationally recognized reports and articles related to voting rights, voting systems and election administration. In April 2009, Mr. Norden completed his duties as Chair of the Ohio Secretary of State's bipartisan Election Summit and Conference, authoring a report that recommended several changes to Ohio's election administration practices and laws; the report was endorsed by most of the State's voting rights groups, as well as the bipartisan Ohio Association of Election Officials. Mr. Norden was the Keynote Speaker at the Sixth Annual Votobit International Conference on Electronic Voting (Buenos Aires, 2008), and the 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (Montreal, 2009). In June 2009, he received the Usability Professional Association's *Usability In Civic Life Award* for his "pioneering work to improve elections." Mr. Norden is the lead author of the book *The Machinery of Democracy: Protecting Elections in an Electronic World* (Academy Chicago Press) and a contributor to the *Encyclopedia of American Civil Liberties* (Routledge 2007).

ACKNOWLEDGEMENTS

As always, the Brennan Center and the author are exceptionally grateful to Laura Seago for putting in many long nights to provide editorial and drafting assistance, as well as ideas that were integral in defining the direction of this report. John Travis performed exceptionally in steering this report to completion. We also thank Susannah Goodman of Common Cause, for pushing us to develop and write this report, and putting us in touch with the many regulatory specialists who reviewed and commented on the ideas in this document. Paul Riley, now at Milbank, Tweed, Hadley & McCloy, provided invaluable research and drafting assistance. Joe Hall, Aaron Burstein, and David Wagner of the University of California at Berkeley and ACCURATE, Flavio Komuves, former Deputy Advocate for the New Jersey Department of the Public Advocate and currently with the ACLU of New Jersey, Justin Levitt, Matt Robinson and Susan Lehman of the Brennan Center and Sean Flaherty, Pam Smith and Warren Stewart of Verified Voting all generously gave many hours to review drafts of this report and provide critical feedback, which has been incorporated into the final document. Thanks also to Scott Kareff of Schulte Roth & Zabel LLP for his careful reviews of this report and his thoughtful feedback.

A special debt of gratitude is owed to Scott Nelson of Public Citizen, who provided us with guidance and insight into how better regulation and oversight could improve voting systems nationwide. We received similarly invaluable assistance from Joan Claybrook, former President of Public Citizen and head of the National Highway Traffic Safety Administration, as well as Pamela Gilbert of Cuneo Gilbert and LaDuca, former Executive Director of the Consumer Product Safety Commission.

Douglas Kellner, co-chair of the New York State Board of Elections, John Gideon, Susan Greenhalgh and Ellen Theissen, among many others, have long advocated for a better clearinghouse for voting system problems, and their perseverance in pushing this idea was an important inspiration for the report.

This report would not have been possible without the many election officials who agreed to be interviewed, review case studies and provide feedback regarding the substance and recommendation of this report. Among the county election officials, we especially thank: Betty McGary, Executive Director, Butler County (Ohio) Board of Elections; Carolyn Crnich, Humboldt County (California) Clerk; Denise Lamb, Chief Deputy Clerk for Elections, Sante Fe County (New Mexico); Cherie Poucher, Director of the Wake County (North Carolina) Board of Elections; Joanne Rajoppi, Union County (New Jersey) Clerk; Rokey Suleman, Executive Director, Washington, D.C. Board of Elections and Ethics; Jane Platten, Director of the Cuyahoga County (Ohio) Board of Elections; Matt Damschroder, Deputy Director of the Franklin County (Ohio) Board of Elections, and Gail Siegel, Communications Director for David Orr, Cook County (Illinois) Clerk. The following state election officials and offices were also exceptionally helpful: Lesley Mara, Deputy Secretary of the State of Connecticut; Lowell Finley, Deputy Secretary of State of California and the office of the Ohio Secretary of State.

We are grateful to the Election Assistance Commission, and in particular, Jeannie Layson, Director of Communications and Congressional Affairs, Matt Masterson, Deputy Director of Testing and Certification Program, and Thomas Wilkey, Executive Director, for graciously agreeing to meet with the author, discuss the ideas in this report, and promptly answer his many questions, as well as the EAC's current efforts to share with state and local election officials important information about election administration and voting systems.

Kitty Garber of the Florida Fair Elections Commission, Professor Penny Venetis of the Rutgers School of Law – Newark, David Zvenyach of the District of Columbia City Council, Professor Candice Hoke, Cleveland Marshall College of Law, and Noel Runyan all provided essential assistance in drafting and reviewing case studies and sidebars integral to this report.

The author thanks Susan Liss, Jeanine Plant-Chirlin, and Wendy Weiser of the Brennan Center for their guidance throughout the drafting process. Of course, any errors in the report are the author's alone.

The Brennan Center is grateful to the Carnegie Corporation of New York, Democracy Alliance Partners, the Ford Foundation, the Irving Harris Foundation, the Mitchell Kapor Foundation, the Open Society Institute, Quixote Foundation, the Rockefeller Family Fund, the Tides Foundation, and two donors who wish to remain anonymous for their generous support of our Voting Rights and Elections Project.

The statements made and the views expressed in this paper are solely the responsibility of the Brennan Center.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Failed voting machines, frustrated voters and lost votes: these have been a constant in news reports following every recent major election cycle. That should not be surprising. The voting systems[1] used in the United States today are complicated machines; each runs on tens of thousands of lines of software code. As with automobiles and airplanes, automatic garage door openers and lawnmowers, occasional malfunctions are inevitable – even after rigorous product testing.

When it comes to system failures, however, voting machines *are different* from automobiles and airplanes, and other products, in at least one important respect: for the vast majority of voting systems in use today, (1) manufacturers are not required to report malfunctions to any government agency, and (2) there is no agency that either investigates such alleged failures or alerts election officials and the general public to possible problems (let alone requires voting system manufacturers to fix such problems).

As this report demonstrates, the consequence of this lack of oversight is predictable. Voting systems fail in a particular county in one election, and then again later, under similar circumstances, but in a different locale. These repeated failures disenfranchise voters and damage public confidence in the electoral system.

The Brennan Center reviewed hundreds of reports of problems with voting systems in the last eight years, and closely studied fourteen of them. Our study shows that election officials and the public are often completely reliant on the private companies that sell and service this voting equipment and related service contracts to voluntarily keep them aware of potential problems with those systems. As one election official we interviewed noted, "vendors are in the business of selling machines, and often don't have an incentive" to inform present and future customers of certain problems with their systems.[2]

The core thesis of this report is simple: we need a new and better regulatory structure to ensure that voting system defects are caught early, officials in affected jurisdictions are notified immediately, and action is taken to make certain that they will be corrected for *all* such systems, wherever they are used in the United States.

Based on our review of regulatory schemes in other industries, we are convinced that the focal point for this new regulatory system must be a clearinghouse – a national database, accessible by election officials and others, that identifies voting system malfunctions that are reported by voting system vendors or election officials. If this database is going to have any real benefit, voting system vendors must be *required* to report all known malfunctions and election officials must have full access to the database.

The Election Assistance Commission (EAC), the relatively new federal agency charged with the task of creating a testing program for new voting system has, within its limited federal mandate, made great strides in the last two years increasing quality control for some of the country's newest voting systems. However, to fully address the problem of underreported and unaddressed voting system problems, the EAC or other federal agency should be given statutory authority and resources to fully implement the kind of database recommended in this report. Such a database would make our electoral system stronger. It would be easier for election officials and others to ensure that their equipment is as user-friendly and accurate as possible. It would also make voting machine vendors more accountable to public officials and taxpayers, incentivizing manufacturers to enhance internal controls. Given the billions of dollars spent by federal and local governments to purchase and maintain new voting equipment over the last several years, this is no small thing.

CORE FINDINGS

Three fundamental findings result from our study of past reported problems, review of current law and contracts for the use and regulation of voting systems, and interviews with election officials:

1. **There is no central location where most election officials can find comprehensive information about problems discovered with their systems before each election.**

    - State and local election officials we interviewed tell us that they must rely almost exclusively on the voting system vendors for information about malfunctions, defects, vulnerabilities and other problems that the vendors have discovered, or that have occurred with their voting systems in other states.

    - A change in election administrators can sometimes mean a loss of knowledge about all of the potential problems with a voting system as well as procedural safeguards necessary to prevent those problems.

    - There are approximately 4,600 separate jurisdictions across the United States that administer elections.[3]

2. **Vendors are frequently under no legal obligation to notify election officials or the public about problems with their systems.**

    - While purchase or service contracts sometimes bind election officials to inform vendors of malfunctions, vendors are not always similarly obligated to inform officials of problems reported to them.

    - Voting system vendors are under no legal obligation to notify any federal agency of problems they discover with the vast majority of their systems in use in the United States today, despite the fact that hundreds of millions of federal dollars have been spent to purchase such equipment.

3. **The same failures occur with the same machines, in one jurisdiction or another, election after election.**

    - Most of the election officials we interviewed in connection with our review of reported problems claimed to have had no prior warning of the issues we discuss. By contrast, in most cases, the vendors were (or should have been) aware of the problems – often because the same problem had been reported to them earlier by another election official.

    - Frequently, these malfunctions – and their consequence, disenfranchisement – could have been avoided had election officials and/or public advocates known about earlier problems and had an opportunity to fix them.

CENTRAL RECOMMENDATION: CREATION OF A NATIONAL DATABASE FOR VOTING SYSTEM PROBLEMS

Given the nature and importance of voting systems to our democracy, we need a new regulatory structure to ensure that voting system defects are caught early, disclosed immediately, and corrected quickly and comprehensively. Accordingly, this new regulatory system must center around a mandatory national clearinghouse, administered by a federal agency empowered to investigate violations and enforce the law.

Based upon our interviews with election officials and regulatory experts, and our review of analogous regulatory structures in other important industries, we conclude that the clearinghouse must include four key elements to work effectively:

1. A Publicly Available, Searchable Centralized Database

Election officials, in particular, would benefit from a publicly available, searchable online database that includes official (i.e., election official-reported or vendor-reported) and unofficial (i.e., voter-reported) data regarding voting system failures, and vulnerabilities, and other reported problems and establishes criteria for the database's contents and organization.

2. Vendor Reporting Requirements

Vendors must be required to notify the appropriate government agency of any known and suspected voting system failures and vulnerabilities, and other reported problems, including customer (i.e., election official) complaints, warranty claims, legal actions and/or actions taken by the vendor to satisfy a warranty or investigate a reported problem.

3. A Federal Agency with Investigatory Powers

The best way to ensure that vendors address potential problems in a timely manner is to empower the appropriate government agency to investigate all voting system failures and vulnerabilities listed on the database, grant the agency subpoena power to facilitate its investigations, and require vendors to, among other things, maintain records that may help the agency determine whether there are indeed voting system failures or vulnerabilities, and whether the vendor has taken appropriate action to address the failures or vulnerabilities.

4. Enforcement Mechanisms

The appropriate government agency must have the power to levy civil penalties on vendors who fail to meet the reporting requirement or to remedy failures or vulnerabilities with their voting systems.

We detail these recommendations more fully on pages 27 - 38 of this report.

ADDITIONAL RECOMMENDATIONS

While a national clearinghouse along the lines we suggest in this report is ultimately the best way to ensure that problems with machines are publicized and corrected throughout the country, there are important interim steps that county and state governments, in particular, can begin taking immediately to increase the chances that election officials are notified of problems with their voting systems and can avoid some of the kinds of problems detailed in this report:

1. Negotiate Better Contracts with Vendors

Provisions in many voting machine contracts make it much more difficult for election officials and the public to get detailed information about system problems reported in other parts of the country, or to hold vendors responsible for problems when something goes wrong. To increase voting system reliability and maximize vendor motivation to minimize the risk of such problems, counties and states should begin demanding certain key contract terms. Pages 39 - 40 of this report discusses these more fully.

This recommendation is particularly relevant to jurisdictions using Premier voting systems. ES&S recently purchased Premier, and pursuant to the proposed Final Judgment for the antitrust action brought by the Department of Justice in March 2010, customers using Premier equipment will have the option of choosing between ES&S and Dominion for future service of those machines.[4] This will provide them with an opportunity to negotiate new contracts.

2. Implement Stronger State Regulation

The legislature in at least one state, California, has passed legislation requiring vendors selling systems within its borders to notify the Secretary of State and all local election officials using its systems of any "defect, fault or failure" within 30 days of discovery.[5] As of the writing of this report, the legislation is currently awaiting a decision by the governor, who had vetoed an earlier version in 2009. In 2005, North Carolina passed a similar bill into law.[6] The California model presents the best legislative attempt we have seen, to date, to address the problems we discuss in this report. We hope more states will adopt this model.

3. Create a Voluntary Database

The appropriate federal agency should create a searchable database to which election officials, vendors, and voters could voluntarily report problems. Absent action by the federal government, a non-governmental organization (like the National Association of Secretaries of State) or even a state government could create such a database.

There would be no way to force vendors to report to this database, or to provide election officials with whistleblower protections for making voluntary reports – two important suggestions for the mandatory clearinghouse detailed in this report – but it could still serve as a useful interim resource for election officials.

4. Pressure Vendors to Voluntarily Post Information on Their Own Sites This Year

One drawback of the three previous recommendations is that they probably cannot be implemented in time for this fall's election. In contrast, vendors could create their own databases relatively quickly, significantly reducing the risk of embarrassing problems. Ideally, vendors would create a central, easily accessible and searchable site where election officials could review all previously issued product advisories, software patches and workarounds, election official complaints, warranty claims, and lawsuits about their systems (together with the result of any vendor investigation, explanations, and actions taken to address these complaints).

County and state officials can and should demand this voluntary action from vendors now, in time to make a difference for November's election.

I. INTRODUCTION

Since 2002, the Federal and State governments have invested billions of dollars in new voting equipment, transforming the way our nation conducts elections and tallies votes. This has had many positive effects. We have replaced many outdated and unreliable systems. Most political scientists agree that the new equipment has dramatically reduced the kinds of voter errors common in Palm Beach County in 2000,[7] and, advances in technology have made it possible for many disabled voters to vote privately and independently for the first time in their lives.

"I ADAMANTLY SUPPORT THE RECOMMENDATION OF THE CREATION OF A NATIONAL, SEARCHABLE DATABASE THAT ELECTION OFFICIALS COULD USE AS REFERENCE TO VOTING SYSTEMS."
JANE PLATTEN, DIRECTOR OF THE CUYAHOGA COUNTY BOARD OF ELECTIONS, OHIO'S LARGEST ELECTION JURISDICTION

But the change has also given an even greater role in our elections to the private companies that manufacture voting machines. The new voting systems run on tens of thousands of lines of proprietary software code. Voting machine vendors create these systems, program, and maintain them. More than ever, election officials and the public must rely on private companies to ensure that citizens' votes are recorded as they were intended to be cast, and that they are counted correctly.

This report details the consequences of lack of regulation and oversight of the voting machine industry. Voting machine manufacturers – unlike many other kinds of manufacturers selling products in the United States – are not required to report malfunctions of most of their systems to any government agency. Nor is there a government agency that either investigates mechanical failures or alerts election officials and the public to possible problems for most systems (let alone requiring voting system manufacturers to fix such problems).

While there has been an increase in government oversight of voting systems in the very recent past – and in particular for new systems introduced since 2009 – we conclude that the current process for publicizing and addressing voting system defects nationally is inadequate.

The Brennan Center closely studied 14 reports of voting system problems during the last few years. In most of these cases, the reported problems resulted in the temporary or permanent miscount or loss of votes. The numbers range from a few dozen to tens of thousands, but in all cases better oversight and reporting requirements could have prevented the problems from occurring at all.

The report that follows is broken into three main sections: first, we describe the law and regulatory structure as it currently exists for addressing voting system failures; second, we document the need to fix this regulatory scheme by providing selected examples of its current failures; and finally, we offer suggestions for changes to the law and regulatory structure that would redress the system's current flaws, based largely on models that have proven successful with other commercial products.

II. THE CURRENT PROCESS FOR PUBLICIZING AND ADDRESSING VOTING SYSTEM DEFECTS

The Help America Vote Act of 2002 (HAVA) resulted in the replacement of voting systems across the country. It also created new standards for the certification and use of these systems. It established the EAC as an independent agency of the federal government and charged it with the task of creating a testing program for the new voting systems and holding hearings and functioning as a clearinghouse for election administration information, among other things.[8] Section 202 of HAVA states in relevant part that "[t]he Commission shall serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal elections . . . ."[9]

Some argue this clearinghouse function should include reporting on the performance of voting equipment purchased with funds granted by HAVA.[10] The EAC has not publicly embraced this interpretation for systems it has not certified, and there is no question that its power to oversee voting system manufacturers has been severely limited by federal statute and resources provided to it.

"A MEANINGFUL AND USEFUL CLEARINGHOUSE FUNCTION IS PARTICULARLY APPROPRIATE AS A FEDERAL RESPONSIBILITY. IT IS MUCH MORE EFFECTIVE FOR A SINGLE FEDERAL AGENCY TO HAVE PRIMARY RESPONSIBILITY FOR IDENTIFYING VOTING SYSTEM PROBLEMS AND TO RECOMMEND REMEDIAL ACTION."
DOUGLAS KELLNER, CO-CHAIR OF THE NEW YORK STATE BOARD OF ELECTIONS

In spite of this, as discussed below, the EAC has recently taken several positive steps to make information about voting system problems more readily available to election officials and the general public. While admirable and important, we believe these steps fall short – both in scope and timeliness – of what is necessary to avoid the kinds of recurring problems detailed in this report. This belief is in no way meant to disparage recent efforts made by the EAC to ensure that problems with its certified systems are tracked and corrected. To the contrary, as discussed more thoroughly in Section IV (*A Better Way to Track and Address Voting System Problems*), current federal law does not allow the EAC or any other federal agency to take many of the steps we recommend to reduce voting system errors. Nor is the EAC or any other federal agency currently provided with funding necessary to take all of the steps we recommend. The EAC's budget in Fiscal Year 2010 was $17,959,000, minus a $3,250,000 pass through to the National Institute of Standards and Technology for a total of just $14,709,000.[11]

The EAC is in the midst of drafting of a new clearinghouse policy,[12] which will be subject to public comment and approval by the EAC's commissioners. Jeannie Layson, Director of EAC Communications and Congressional Affairs, has recommended a pilot program limited in scope and duration to allow the EAC to determine resources needed to operate the new clearinghouse.[13] The Brennan Center has asked the EAC to comment on the extent of its powers and obligations under the clearinghouse provisions of HAVA. The EAC has declined to state whether its new clearinghouse policy will require more reporting on the performance of voting equipment purchased with HAVA funds pending final adoption of that policy.[14] However, in the past, the EAC has taken the position that it does not have the authority or resources to track and resolve problems associated with voting systems it has not certified[15] – which, as discussed below, represents nearly all of the voting systems in use in the United States today.

Separate and apart from its soon-to-be released clearinghouse policy, the EAC has recently adopted a number of important reporting requirements for both voting system manufacturers and testing labs that participate in

its newly established Voting System Testing and Certification Program.[16] Pursuant to the Quality Monitoring Program established in the Voting System Testing and Certification Program Manual (the "VSTCPM") the EAC will post on its website "test reports" for all systems tested for EAC certification, regardless of whether or not they are ultimately certified. These test reports will include a list of "discrepancies" identified during the testing.[17] It will also post information related to site audits that it conducts on manufacturers who participate in its program.[18]

Under the VSTCPM, vendors must report to the EAC "malfunctions" of *EAC certified* systems. The VSTCPM defines "malfunction" as "a failure of a voting system, not caused solely by operator or administrative error, which causes the system to cease operation during a Federal election or otherwise results in data loss."[19] The EAC will also post this information on its website. The EAC recently informed the Brennan Center that it intends to post a map showing all jurisdictions that use EAC certified systems, with links to all vendor reported anomalies for such systems.[20] Finally, of relevance to this report, election officials may voluntarily report "anomalies" for such systems if they result "in some disruption to the election process," provided the election officials provide their name, title, and jurisdiction, among other information.[21]

This new system had two recent important public successes. The first occured on June 25, 2010, when the EAC put out a "Voting System Technical Advisory" (VSTA) for the ES&S Unity 3.2.0.0 system, which has been certified by the EAC. The advisory came two months after Jane Platten, Director of the Cuyahoga County Board of Elections, notified the EAC that during testing of the machines prior to a May primary election, approximately 10 percent of the machines started powering down and then freezing.[22] After extensive consultation with both ES&S and Cuyahoga County, the VSTA was sent to election officials using the same system, advising them what steps to take in the event this freeze or power failure occurred during opening or closing of the polls, or during voting.[23]

On August 23, 2010, the EAC issued a VSTA for the MicroVote EMS 4.0B, noting that the voting panel for the system's Direct Recording Electronic device would not operate with certain flash cards.[24]

While the recent steps by the EAC are unquestionably valuable, there are a number of factors which limit the usefulness of this reporting system. They are discussed in greater detail in Section IV (*A Better Way to Track and Address Voting System Problems*) of this report. A summary of some of the most serious limitations of the current system follows:

- Perhaps most importantly, the EAC only certified its first voting system in February 2009 – meaning that almost none of the machines currently in use in the United States are covered by VSTCPM reporting rules, or any federal reporting requirements, for that matter. Of the approximately 4,600 election jurisdictions in the United States, we are aware of *only a few dozen*[25] *that will use EAC certified equipment in 2010.* In other words, approximately 99 percent of U.S. jurisdictions in 2010 will be using equipment that is not certified by the EAC and therefore not covered by this program.

- As most polling place equipment in use in the United States was purchased after 2002, and because many jurisdictions replacing equipment are likely to continue to use non-EAC certified equipment in the future, we expect it could be decades before even a large majority of jurisdictions in the United States are using EAC certified systems.[26] In fact, only *twelve states* require federal certification for new systems, so – absent changes at the state level – it is not certain that the EAC's program will ever cover most jurisdictions in the United States.[27]

- Mandatory reporting by vendors is required only if the EAC-certified system "malfunctioned" during a federal election. Thus, if a vendor becomes aware of a problem that occurred when there were no federal candidates on the ballot, it is apparently under no obligation to report the problem to the EAC.

- Reporting under this system is limited to vendors and election officials for a very specific type of problem. For instance, it is not clear that manufacturers would have to report potential flaws they discover before they result in actual loss of votes on Election Day, or "merely" because they cause delay and long lines rather than a loss of data.

- Independent investigators and voters with credible reports, no matter how numerous or serious, are not entitled to report problems.

- Even where county election officials voluntarily provide anomaly reports (exposing themselves to potentially unhappy vendors, as discussed on pages 25 - 26), the EAC is not required to provide this information to other users of such systems unless various criteria are met, including verification from "the relevant State's chief election official."[28]

- Some election officials have complained that neither the EAC nor the vendors are required to notify election officials immediately upon learning of a malfunction. Douglas A. Kellner, co-chair of the New York State Board of Elections, in a letter to the EAC praising them for issuing their first Voting System Technical Advisory last June, noted that it came two months after the EAC was first notified of the problem and urged "the EAC to put in place a system that would allow an immediate preliminary notice to be distributed to all jurisdictions using the equipment involved as soon as EAC staff has been able to verify a report."[29]

For these and other reasons, most state and local election officials we interviewed tell us that they must still rely almost exclusively on the voting system vendors for information about malfunctions, defects, vulnerabilities and other problems that the vendors have discovered, or that have occurred with their voting systems in other states. Vendors are frequently under no legal obligation to provide such information. While purchase or service contracts sometimes bind election officials to inform vendors of malfunctions, vendors are not always similarly obligated to inform officials of problems reported to them.[30] As Jane Platten put it, "One of the more frustrating aspects of encountering problems [with voting systems], often while preparing and testing for elections as well as on election day or during tabulation, is that the vendors themselves often know about the problems and never disclose any details whatsoever prior to the moment of crisis."[31]

Of course, vendors do frequently notify election officials of problems when they occur, and often provide software patches or other procedural safeguards to ensure that such problems do not occur in the future. Unfortunately, in at least some instances, vendors have appeared slow to acknowledge such problems.[32]

More to the point, there is no centralized location where election officials can find information about anomalies, malfunctions, usability concerns,[33] and other problems discovered with systems they are currently using before each election. A change in election administrators can sometimes mean a loss of knowledge about all of the potential problems with a voting system as well as procedural safeguards necessary to prevent those problems.[34]

The result, as this report demonstrates, is that all too frequently the same failures in the same voting systems occur in one jurisdiction or another, election after election. Often, these malfunctions – and their consequence, disenfranchisement – would have been avoided had election officials and/or public advocates known about previously encountered problems and had an opportunity to fix them.

III. FAILURES OF THE CURRENT SYSTEM: CASE STUDIES

Press reports from the last several years contain hundreds of reported cases of voting machine malfunctions. A subset of these cases is summarized in Appendix B of this report (available in the online version of this report). News items about voting system troubles tend not to include many details; this makes it hard to identify from these reports the precise cause of a particular malfunction. Whatever the causes of a particular problem, it is fair to assume that their occurrence in one jurisdiction will often eventually be repeated in another unless election officials throughout the country are made aware of both the causes of the problem and how to avoid them.

Of the hundreds of reports of voting system malfunctions and vulnerabilities, we collected and closely studied fourteen. They are summarized below. Most of the election officials we interviewed in connection with these summaries claimed to have had no prior warning of the problems we discuss. By contrast, in most cases, the vendors were (or should have been) aware of the problems – often because the same problem had been reported to them earlier by another election official.

"ONE OF THE MORE FRUSTRATING ASPECTS OF ENCOUNTERING [VOTING MACHINE] PROBLEMS . . . IS THAT THE VENDORS THEMSELVES OFTEN KNOW ABOUT THE PROBLEMS AND NEVER DISCLOSE ANY DETAILS WHATSOEVER PRIOR TO THE MOMENT OF CRISIS."
JANE PLATTEN, CUYAHOGA COUNTY BOARD OF ELECTIONS

1. Butler County, Ohio, March 2008

In March 2008, as they reconciled vote totals from the State primary in their office's Data Department, Ohio officials noticed that several votes were dropped from memory cards even though their final report stated that votes on these memory cards were counted.[35] A subsequent investigation by Ohio election officials determined that at least 1,000 votes were undercounted in nine of Ohio's forty-four counties using Premier touch screen or optical scan voting systems.[36] In an editorial several months later, the *New York Times* noted that Premier (known as Diebold Election Systems prior to rebranding in 2007) had subsequently notified more than thirty states using its systems "to be on the lookout for missing votes."[37]

Less widely reported was the fact that this same problem was apparently discovered in DuPage County, Illinois in 2004. In a county election summary (obtained by the Illinois Ballot Integrity Project and the relevant portions of which are annexed to this report as Appendix C), a technician who serviced the machines noted what appears to be the very same problem:

> *GEMS Upload Failure on York 58* – This memory card had a failed upload transmission on election night that was not detected until the next day when reports were on the precinct, and zero results were found for each race within the precinct. The status of the memory card upload within the GEMS was "successful" but the upload record showed the ballot count to be zero. It is rather discomforting [sic] that this failed transmission was not detected on election night.

The publicity around the problems in Butler County, Ohio in March 2008 may have saved thousands of votes on Election Day the following November. It is impossible to know how many votes were lost before the problem was so widely publicized.

Nor was the mere reporting of the problem to the vendor in 2008 enough to guarantee that the 29 other States using this system that year would have known how to protect themselves from similar problems. As the rest of this case study shows, it was the extreme vigilance of the Butler County Board of Elections and the Ohio Secretary of State that resulted in the full scope of the problem being revealed.

On April 4, 2008, the Butler County Board of Elections sent a letter to Premier and copied the Secretary of State, Jennifer Brunner, notifying Premier of the problem.[38] The Board sent a follow up letter to Premier on April 9, 2008 notifying them of a recurrence of the problem.[39]

On May 16, 2008, in response to Butler County's complaint, Premier issued a report that blamed the problem on antivirus software the county had run on their system as well as human error.[40]

County Election Director Betty McGary reports that on May 23, she wrote to Dave Byrd, President of Premier, calling their report "highly speculative," and rejecting their assumptions. She states that she requested Premier continue to research and diagnose the root source of the discrepancies.[41]

Had Butler County's Board of Elections been less persistent, that might have been the end of the story. Other election officials using this system around the country might not have learned of the problems experienced in Butler County, and almost certainly would not have discovered its true cause.

Fortunately, the Butler County Board asked the Ohio Secretary of State's office to assist it in its own investigation of the problem. On August 6-7, 2008, Butler County election officials and the Ohio Secretary of State conducted a simulation of the vote counting process with Premier observers. They conducted eight of these simulations over two days – in some cases disabling the antivirus software Premier had blamed for the malfunction, in other cases enabling it.[42]

The testing revealed that the machines dropped votes during multiple memory card uploads from individual voting machines onto the county server regardless of whether the antivirus software was enabled.[43]

After the testing, Premier conceded that the apparent root cause for the problem was an error with their server software, which the company determined "contains a logic error" that can sometimes result in dropped votes from a sharing violation when multiple cards from individual machines were uploaded at the same time.[44]

Following its additional investigation, Premier sent a product advisory to all counties using its systems detailing procedures intended to "mitigate and reveal this issue should it occur."[45]

Director McGary supports a mandatory requirement for "voting machine vendors to report all malfunctions and complaints they receive from election officials to a central and searchable database," noting that "such reporting should be mandatory."[46]

2. Humboldt County, California, November 2008

In November 2008, election officials in Humboldt County, California implemented a post-election "Transparency Project," whereby a separate scanner not manufactured by the voting machine vendor electronically counted every paper optical scan ballot during the election. The purpose was to verify the official vote totals and to post ballot images on the internet in order to allow any member of the public to conduct independent recounts.[47]

The Transparency Project turned up a counting error on Humboldt County's voting machines: they failed to count approximately two hundred ballots.[48] According to Humboldt County Clerk Carolyn Crnich, the first batch of absentee ballots scanned into the voting system, known as "deck zero," disappeared from the totals produced by the voting system before officials finished scanning all of the ballots and certified the vote totals.[49] Upon learning of the problem, Crnich contacted the voting system vendor.[50]

WIRED AND COMPUTERWORLD MAGAZINES HAVE REPORTED THAT THE VOTING SYSTEM VENDOR WAS AWARE OF THE "DECK ZERO" PROBLEM FOR YEARS, BUT DID NOT NOTIFY THE ELECTION ASSISTANCE COMMISSION, THE NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS, OR THE CALIFORNIA SECRETARY OF STATE, CALIFORNIA'S CHIEF ELECTION OFFICIAL.

Crnich states that after examining copies of the county's database, the vendor told her that a programming error in its election management system, the software used to aggregate the votes from all of the county's voting machines, caused the problem.[51]

Wired and *Computerworld* magazines have reported that the voting system vendor was aware of the "deck zero" problem for years, but did not notify the Election Assistance Commission, the National Association of State Election Directors, or the California Secretary of State, California's chief election official.[52] Instead, according to a report issued by California Secretary of State Bowen after the Humboldt County incident came to light, the vendor sent "a vague e-mail to election officials" in California that used the software with the programming problem, recommending a "workaround" procedure without identifying the problem or the potential consequences (i.e., lost votes) of failing to implement the workaround.[53]

The voting system vendor has testified that once it first identified the software problem in October 2004, it "communicated" its findings, and "a simple procedure workaround to mitigate this issue, via email to all California counties then affected."[54] Carolyn Crnich does not dispute that the vendor may have informed her predecessor of the problem. She is certain, however, that her predecessor did not leave any documentation about the problem when she took over, or institute procedures that would have prevented the problem from causing the voting system to lose votes.[55]

Nor did the vendor report the problem to the California Secretary of State's office. As the vendor noted in testimony, at the time there was no "mandate for reporting issues of this nature" to the Secretary of State.[56]

Humboldt County Election Director Crnich has stated that if there were an EAC database with information detailing problems that other counties had experienced using the same voting system used in Humboldt County that she could have accessed before the November 2008 election, she almost certainly would have used it. Such a database would have alerted her to the programming issue with her county's tally server, as well as the workaround. Crnich stated that she believed it was well within the EAC's mandate to provide this kind of information to local election officials and that new officials, who might have little experience with the systems they are charged with using, would particularly benefit from this kind of database.[57]

3. Orange County, Florida, November 2006

In 2007, the Florida Division of Elections listed Orange County as experiencing the highest undervote rates in the state on absentee ballots cast in the 2006 general election for both the U.S. Senate race and the state Governor's race.[58] Alarmed by the exceptionally high rate of undervoted ballots in a major election – nearly 5 percent – the Florida Fair Elections Center's Associate Director contacted the Orange County Elections Administrator, who promised to investigate the issue.[59] According to the Center, Orange County officials responded to the inquiry by stating that their manual inspection of the ballots confirmed that some legitimately cast ballots had not been counted. The Center adds that when they questioned the vendor of the county's OpTech optical scan machines about the problem, the vendor's representative identified the problem as the scanners' failure to read certain types of gel ink used by voters to complete their ballots.[60]

On further investigation, the Center discovered that the same problem seemed to have occurred on similar scanning equipment in March of 2004 in Napa County, California. In that election, optical scanners manufactured by Sequoia failed to count some ballots voted with gel ink.[61] This problem was only discovered during the state's legally-mandated hand count of 1 percent of the ballots cast in the election.[62] Sequoia told *Wired* magazine that the problem was not with the machines themselves, but rather with the county's calibration procedures – the machines were calibrated to read only carbon ink, not dye-based ink found in many gel pens.[63] According to Sequoia, the issue could have been avoided through more thorough pre-election testing.[64]

When the Florida Fair Elections Center delved more deeply into the history of this type of problem, they learned that in the 2000 election, Orange County's optical scan machines failed to count more than 400 votes in the presidential race for no apparent reason.[65] At the time, it was postulated that one possible explanation for the machines' failure to count these ballots was "low carbon content in the ink pens used to mark them."[66] Kitty Garber, Associate Director of the Center, believes that both the vendor and the state were well aware of this before the time she discovered the issue in 2007 – in part because the vendor so quickly identified the source of the problem. For some reason, she states, this was not adequately "communicated to the people actually running the elections" in Orange County in 2004 or 2006.[67]

Bill Cowles, Supervisor of Elections for Orange County noted in an interview with us that the county switched to a different model of ES&S scanner after the 2006 general election.[68] Florida has also implemented a post-election audit law in the intervening years, though a 2008 study by the Brennan Center and others has been critical of that audit as being insufficiently robust to catch many problems.[69]

4. Pulaski County, Arkansas, May 2006

During early voting in the May primary, several voters complained of problems with an ES&S touch screen DRE.[70] According to a local newscast, Pulaski County election officials tested the machine and determined that the machine was not broken; an optical illusion perceived by voters who were over six feet tall caused the problem.[71] Officials determined that the angle at which particularly tall voters viewed the screen caused them to believe that they were voting for the candidate below the one for whom a vote was recorded.[72] This is a significant problem given that more than 15 percent of American males over the age of 20 are six feet tall or taller.[73]

Pulaski County Director of Elections Susan Inman told the *Arkansas Democrat-Gazette* that when she asked ES&S to examine the machine to ensure that there wasn't a problem with the equipment, a company employee told her that they were already aware of optical illusion problems experienced by tall voters.[74]

A review screen that appears before voters finalize their ballots alerted some to the fact that their votes were not recorded as intended. However, several studies have shown that most voters will not notice errors on their final review screens, so there is no way to know how many voters in Pulaski County actually cast their ballots for candidates other than the candidate of their choice.[75] Officials were livid at the thought that ES&S could have known about the problem and failed to warn them.[76] Pulaski County Prosecuting Attorney Larry Jegley launched an investigation into the issue, saying, "I can't understand how in the world a big company like ES&S, with contracts all over the state of Arkansas, would know about a problem like this and fail to fix it."[77]

• • •

5. Florida, November 2006

In 2007, Diebold, Inc. conceded that its optical scan readers had a glitch that caused memory card failures, and told the *Daytona Beach News-Journal* that it would investigate the "J40 connector" that attaches memory cards to its optical scan voting machines.[78] This admission came after complaints about memory card failures from election officials dating as far back as 2000.[79]

According to the *News-Journal*, Volusia County, Florida reported that eleven memory cards in Diebold optical scan machines failed during the November 2006 general election.[80] Premier told the *News-Journal* that the 4.4 percent error rate in Volusia County was "unusual," but an investigation by the paper revealed even higher error rates in other Florida counties using the same equipment.[81] According to public records obtained by the paper, several other Florida counties experienced failure rates that were comparable to or higher than those observed in Volusia County.[82]

The 2006 incidents were not the first time that memory cards in Diebold machines failed in Volusia and other Florida counties. According to the *News-Journal*, a 2004 county report indicates that Volusia had 57 memory card failures, which Diebold stated was "more memory card failures than 'the rest of our customers in Florida combined.'"[83] The paper also reported that Volusia's problems with memory cards dated back to the 2000 general election, when 300 ballots went uncounted when a memory card failed in the middle of ballot scanning.[84] The loss of votes was not discovered until a hand recount began as a result of the close contest.[85] The *News-Journal* noted that "Volusia County's most infamous memory card problem . . . when more than 16,000 negative votes were recorded against Al Gore," had "never been determined." At the time, a county election official wrote an angry e-mail asking the manufacturer to "please explain this so that I have the information to give the auditor instead of standing here looking dumb."[86]

Despite this long history of failures with the same equipment, state election officials said in 2007 that they were previously unaware of the problem.[87]

By 2007, nearly 25,000 Diebold optical scans machines were in use nationwide. The *News-Journal* reported that the manufacturer conducted a survey of its customers to determine the frequency of such failures, but refused to release results from the study, calling it proprietary information.[88] According to the *News-Journal*, officials at the Election Assistance Commission told the paper that they could not compel distribution of this information unless an official government agency requested the action.[89] Many saw this as an argument for the EAC to bolster its clearinghouse function. "[T]he federal agency required by law to act as a clearinghouse on voting system problems – the U.S. Election Assistance Commission – has been slow to develop a place where such information can be shared," the *News-Journal* reported in 2007, "The [election] supervisors are left largely on their own."[90]

• • •

6. Broward County, Florida, November 2004

Two days after Election Day in November 2004, Broward County election officials double-checked election results and discovered that tens of thousands of votes on certain state amendments were not counted. The problem: a "software glitch" in the system used to count the county's absentee ballots.[91] According to the *Palm Beach Post*, the software started counting backward after it logged 32,000 votes in a race.[92] Once officials identified the problem and obtained correct vote totals, the newfound votes contributed to a changed result for a statewide gambling amendment and sparked angry calls for a recount. [93]

THE NEWS-JOURNAL REPORTED THAT DIEBOLD CONDUCTED A SURVEY OF ITS CUSTOMERS TO DETERMINE THE FREQUENCY OF SUCH FAILURES, BUT REFUSED TO RELEASE THE RESULTS, CALLING THEM PROPRIETARY.

Several newspapers reported that ES&S, the voting system vendor, claimed to have noticed the problem in 2002, and said it notified the Secretary of State's office of the issue after that election.[94] It isn't clear from news accounts why Broward County did not adopt procedures to safeguard against this glitch once it was discovered. Broward County officials told the *Palm Beach Post* that the manufacturer claimed its upgrades were rejected by the Secretary of State's office in 2002; the state contested this claim.[95] One reason officials in 2004 may have been unaware of the problem: there was turnover in the offices of chief election officials in both Broward County and the State of Florida between 2002, when the software glitch was originally discovered, and 2004, when the unaddressed problem caused Broward County to miscount the votes.

Regardless of who was to blame for Broward County's failure to address the problem ahead of time, a centralized database could have prevented it, by allowing Broward County officials in 2004 to review reported problems for their systems, including necessary workaround procedures, and avoid the controversy that followed the well-publicized tallying problems.

7. Florida, June 2004

According to the *Miami Herald*, only five months before the 2004 general election, some state officials learned that touch-screen voting machines used in 11 of the state's counties contained a software flaw that would make it impossible to conduct a manual recount of ballot images in close races.[96] Election officials in at least one Florida county knew about the problem as early as 2002, but for whatever reason, the existence of the flaw was not understood by the relevant State election officials for nearly a full year.[97]

Miami-Dade County learned of the problem after an election in May 2003. The division director of the County's technology department found that the electronic event log of voting activity scrambled the serial numbers of voting machines.[98] He wrote a letter to the County elections supervisor on June 6, 2003 stating that "I believe there is a serious 'bug' in the program(s) that generate these reports, making the reports unusable for the purpose that we were considering (audit an election, recount an election and, if necessary, use these reports to certify an election)."[99]

The vendor of the machine assured all parties that the software flaw would not affect the counting of votes. Nevertheless, there was concern that if counties were ordered to produce a record of the votes in a close race for the purpose of conducting a recount, some of the relevant data could be lost.[100]

Press reports indicate that, at least initially, the media attention to the flaw in June 2004 led to a round of finger-pointing among Florida election officials, with the Florida Secretary of State "blasting" Miami-Dade officials for failing to notify her office when they learned of the problem a year earlier, and Miami-Dade officials, arguing that other counties that discovered the same problem should have notified the state, to put more pressure on the vendor to "come up with a so-called work-around to the problem before the mistake was repeated."[101]

Again, a centralized database that listed reports of problems from vendors and election officials would probably have provided election officials in Florida with much earlier notice of the problem.

• • •

8. Alameda and San Diego Counties, California, March 2004

According to the *San Diego Union-Tribune*, on the morning of the March 2 primary election, more than 700 Diebold precinct control modules that activate the cards used to call up ballots on touch screen machines displayed the wrong start-up screen.[102] With no way to load ballots onto the voting machines, hundreds of polling sites had to delay opening their doors, some by as much as three hours.[103] Some voters told the *Union Tribune* that they had to leave before getting the opportunity to cast a ballot.[104]

Shortly after the primary, a Diebold spokesman acknowledged that the start up screen on precinct control modules could fail in the event of a problem with the unit's power supply, calling the glitch "a possibility […] but it was an improbability."[105] A report released by the company six weeks later revealed that the problem was caused by faulty power switches that failed to fully turn off the units when placed in the 'off' position, causing power to drain from the machines before election day.[106]

The Secretary of State's Voting Systems and Procedures Panel called a hearing in late April to examine the problems experienced during the primary. At the hearing, former Diebold technician James Dunn testified that the problems with batteries losing power were evident before the machines were shipped to San Diego and Alameda counties.[107]

The technician, whose job was to assemble voting machines, load their software, and pack them for shipment, testified that battery problems could lead to incidents like those seen on primary day:

> We had a significant amount of problems with the batteries. In fact, one of the things we were told – one of the last things we were to check was before they packed up, was that they were supposed to have 60 to 70 percent battery load in them due to the problem of the batteries discharging once they reached anywhere from 20 to 15 percent charge rate, they would then dump the settings, sometimes dump the software load, and then on initial startup, would being up a standard Windows CE screen and not the Diebold screen … [This occurred] [f]requently. All the time.[108]

Calling the disaster in San Diego and Alameda counties "predictable" and the problem "fully known," Mr. Dunn testified that he notified supervisors of the problem and was told that the company knew that machines encountered this problem once the batteries discharged to a certain point, and that their solution was simply to ensure that the machines were shipped with a sufficient charge.[109]

At the hearing, an attorney for Diebold contested the accuracy of Mr. Dunn's testimony in vague terms, but of the battery problems on Election Day, company president Robert Urosevich said, "We were caught. I apologize for that."[110]

• • •

9. Bernalillo County, New Mexico, November 2002

Ten days after Election Day in 2002, Bernalillo County Commissioners discovered that their electronic voting system reported approximately 36,000 votes even though nearly 48,000 voters had signed in at the polls. As reported in the *Albuquerque Tribune*, the vice president and regional manager of the voting system vendor stated that the individual touch-screen machines recorded the votes correctly, but the "software program used to [aggregate] all the votes," did not have the capacity to handle the totals and was "overwhelmed by the data."[111] The result was that nearly 12,000 votes were missing from the totals produced by the voting system.

In fact, the very same problem occurred weeks earlier in Clark County, Nevada and was fixed for future elections.[112] Unfortunately, according to the *Albuquerque Tribune*, the technician in charge of Bernalillo County's problems was not told of the Clark County problems, and was not provided with the patch.[113]

James Noel, who served as counsel to one of the candidates on the ballot that day, discovered the problem several days after the election.[114] According to Mr. Noel, as he reviewed the unofficial results, he noticed undervote rates of 20 to 25 percent for the early voting period for statewide and federal offices. This was higher than the undervote rate in down-ticket races, not something that one would typically expect. He estimated that thousands of votes might not have been counted.[115]

Mr. Noel stated that he brought this anomaly to the attention of the County Clerk, and that despite this fact, she recommended final certification of the results several days later.[116] Mr. Noel objected to certification, pointing out the unusually high undervote rate in statewide and federal races, and the board voted to delay certification pending investigation by the County Clerk.[117] When told of the problem, the vendor re-ran the results "using the software patch this time," and issued a new report that included the missing ballots.[118]

Denise Lamb, who currently serves as Chief Deputy Clerk for Elections in Sante Fe County, New Mexico, believes that a central database that detailed malfunctions for each system, as well as workarounds or software patches supplied by the vendors, could have prevented the problems that Bernalillo County encountered with its tally server in 2002, and certainly would have allowed the County to understand quickly the potential source of the malfunction once it occurred. She noted that, "vendors are in the business of selling machines, and often don't have an incentive" to inform present and future customers of problems with their systems.[119]

• • •

10. Wake County, North Carolina, November 2002

According to *Wired News*, ES&S discovered a glitch in the firmware of its touchscreen voting machines used during early voting in the 2002 general election in Jackson County, North Carolina.[120] The glitch "made the ES&S machines falsely sense that their memories were full," a company spokeswoman told the magazine.[121] The potential result of this error was that memory cards associated with the machines would not record votes that had been cast. Fortunately, the problem was fixable.[122]

DENISE LAMB, WHO CURRENTLY SERVES AS CHIEF DEPUTY CLERK FOR ELECTIONS IN SANTE FE COUNTY, NEW MEXICO, NOTED THAT, "VENDORS ARE IN THE BUSINESS OF SELLING MACHINES, AND OFTEN DON'T HAVE AN INCENTIVE" TO INFORM PRESENT AND FUTURE CUSTOMERS OF PROBLEMS WITH THEIR SYSTEMS.

Election officials in neighboring Wake County later found this same glitch "by chance" during their own early voting period that year.[123] Election officials told *Wired* that at the time, early voters would fill out paper applications which contained tracking numbers. Each application had a tracking number, and before the early voters cast their votes on the touch-screen machines, poll-workers typed the number into the machines. At some point, election officials compared the number of votes on the machines to the applications, and found that the two figures did not match.[124] As the Brennan Center and other organizations have documented, even today many election jurisdictions do not always follow such reconciliation practices.[125]

According to Cherie Poucher, Director of the Wake County Board of Elections, upon learning of the discrepancy, she immediately contacted ES&S. She says that at that point, she was told that Jackson County had experienced a similar problem. Poucher stated this was the first time she had been informed of this problem.[126]

Ms. Poucher stated that in all, six touch-screen voting machines used in Wake County had lost 436 ballots as a result of the problem. Because the county had paper applications and a numerical code associated with the lost votes, they were able to contact voters whose votes had been lost, and provide them with the opportunity to revote. Many did so.[127] Unfortunately, as Professor David Dill of Stanford has noted, we can't be sure "that other counties didn't lose votes that they didn't catch."[128]

ACCESSIBLE VOTING SYSTEMS

The Help America Vote Act (HAVA) requires that every polling place used for federal elections be equipped with a voting system that is "accessible for individuals with disabilities . . . in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."[129] Many disability rights advocates rightly hail this provision of HAVA as a civil rights milestone, providing millions of Americans with the opportunity to vote privately and independently for the first time in their lives.

Unfortunately, however, reports indicate that accessible systems too often malfunction on Election Day, frustrating voters with disabilities.[130] As a result, HAVA's mandate has sometimes gone unfulfilled, and these voters have been forced to either seek assistance and lose their privacy while voting, or to give up on voting in their polling places altogether. Over the past several years, there have been several individual[131] and institutional[132] reports detailing problems that voters with disabilities have experienced using these systems.[133] They have included audio keypads and output that failed to work, VVPAT printers on accessible units that malfunction, and accessible machines that cannot read ballots correctly. Frequently these "malfunctions" could have been avoided if poll workers or election officials were aware of procedures to prevent them.

The appendix available in the online version of this report details some of the defects that have threatened to disenfranchise voters with disabilities, but a comprehensive collection of reported malfunctions in accessible voting systems does not exist in one location. There is no easy way for election officials, disability rights advocates or voters with disabilities to review a comprehensive list of problems associated with these systems, or the countermeasures that election officials can implement to avoid them.

A centralized database that allowed users to search these kinds of problems could greatly improve the voting experience of voters with disabilities. Such a database would not prevent malfunctions. But it would give election officials significant knowledge, so that they could take steps to prevent malfunctions, or quickly correct them. It would also give election officials – and voters – the opportunity to warn their counterparts in other areas of the country about problems experienced in various polling places with accessible units and to remedy such problems prior to Election Day.

Ms. Poucher has stated that it "would be fantastic" if the EAC or other federal agency would establish a searchable database that would allow election officials to see what kind of problems other jurisdictions around the country had with the same systems she was using, whether the vendor had provided them with patches or other fixes, and what procedures they were using to prevent similar problems in the future.[134] She noted that if she discovered a problem during a small, off-year election, it might draw little notice in her own county, but an EAC database would provide her with an opportunity to inform other election officials throughout the country using the same system of the malfunction, and prevent more damaging problems down the road. "I think this kind of database would get integrity back in the system," she added.[135]

Additional case studies further suggest that vendors are too often slow to acknowledge problems with their systems and frequently do not cooperate as fully or as transparently as public officials (and members of the public) would like when problems are confirmed. At the same time, because the last few years have seen a number of voting system vendors go out of business or get bought out by rivals, election officials may not have *any* vendor to turn to for explanation when a problem occurs (see Case Study 11 below and *The Suboptimal Structure of the Voting System Market* at pp. 25 - 26). This is why we believe it is critical that vendors be *required* to report problems to the clearinghouse within a certain time period when certain events occur.[136]

• • •

11. Fairfax County, Virginia, March 2009

In March of 2009, during the post-election canvass for a closely contested special election to fill a vacancy for the County Board of Supervisors, election officials and observers noticed that the combined totals for two AVC WinVote DRE voting machines in a precinct showed a total of 359 votes cast, with 377 votes recorded for the Republican, 328 for the Democrat, and eighteen for other candidates, for a total of 723 votes – or 364 more votes recorded than cast.[137] Officials in Virginia were lucky to catch this problem. As the Brennan Center and others have shown, several jurisdictions in the United States have inadequate ballot accounting and reconciliation practices.[138] In such cases, it is possible to miss this kind of error.

The post-election canvass showed that while one machine recorded 723 votes, only 707 voters had signed-in to that precinct on Election Day, and 348 votes had been cast and correctly counted on another machine in the same precinct. Election officials decided to print the "ballot images" (or the software's digital representation of the ballots cast by voters), and add those up by hand. When they did that, the number of votes on the two machines combined equaled the number of voters who checked in at the polls, and for each machine the number of voters equaled the sum of the number of votes for each candidate. It was only by checking the number of votes against the poll books and by using an alternative method of vote counting that officials were able to determine the result with some certainty. It is important to note, however, that while the ballot images correlated with the number of voters who used the machine, the WinVote does not produce a paper trail; the ballot images are created by the voting system itself, not by voters.

While Fairfax County officials were satisfied that ballot accounting redundancies allowed them to determine accurate election results, they were never able to determine the cause of the problem with certainty.[139] They surmised that the problematic machine did not reset properly after pre-election testing, but they are not sure why this occurred in 2009 after years of using the same machines without

incident.[140] Because the manufacturer of the system was no longer in business, the county had to track down a programmer familiar with the system to corroborate its theory.[141] County Election Manager Judy Flaig acknowledges that conducting the type of investigation necessary to determine the cause of the problem to even this limited extent would not have been possible for every county, and that as much as jurisdictions try to communicate with manufacturers and one another, some information falls through the cracks."Most jurisdictions don't have the resources to do this kind of work," Flaig said, "something like [a database of voting machine problems] would really be helpful."[142]

Rokey Suleman, Fairfax County Registrar at the time of the incident, says he still does not know what caused the problem. Although he no longer works in Fairfax County, he believes other officials using these machines "should certainly want to know what happened, so that they can put the proper procedures in place to ensure it doesn't happen again."[143]

Hinds County, Mississippi also uses the AVS WinVotes. Suleman noted that "unless they read a tiny Vienna, Virginia newspaper where this story was reported, there's no way they would know about this problem."[144] Indeed, the Brennan Center contacted Hinds County Supervisor Robert Graham, and he had never heard of the problems in Fairfax County.

Suleman, who is now the Executive Director of the District of Columbia's Board of Elections and Ethics, noted that in addition to providing election officials with notice of potential problems with the machines they are using, a central database would have other benefits for election officials. Mr. Suleman stated that Washington, D.C. "just went through a procurement process for new voting machines," and that he would have been greatly helped by a central database that could "serve as a repository to let me know what issues exist with the machines, rather than having to rely on what the vendors spoon-feed me."

• • •

12. District of Columbia, September 2008

A District of Columbia Council investigation after the District's 2008 primary found that vote totals originally produced by a Sequoia tally server on election night were "obviously inaccurate."[145] The Board of Elections traced the problem to a cartridge for a Sequoia precinct-count optical scanner in one precinct, which reported voter turnout nearly twice that of the registered population of the precinct and showed 1,554 write-in votes in a race without a write-in campaign.[146] In two reports in the *Washington Post*, election officials indicated that the malfunctioning cartridge caused other problems with the preliminary vote totals.[147] According to acting Executive Director of the D.C. Board of Elections Sylvia Goldsberry-Adams, "one defective cartridge caused vote totals to be duplicated into multiple races on the summary report issued by our office;" on this summary report, 1,542 appeared as the number of overvotes in five contests.[148]

The District Board of Elections asked Sequoia to explain the problems. In an initial response, Sequoia stated that it found "no anomalies or irregularities in either the data or the internal event logs that can be identified as having caused or contributed to the issue experienced on election night."[149] In response to the Board's request for a more detailed explanation, Sequoia issued a report that attributed the problem to human error and ruled out "[e]ndemic hardware and software failures […] as the cause."[150] As for the Board's request for information about past occurrences of this error, Sequoia responded, "[s]ince our customers conduct the actual elections – not Sequoia – we do not have any way of keeping track of such incidents, *nor is it our responsibility to do so.*"[151]

Sequoia identified four possible causes for the problem, including a transient malfunction of the memory pack reader, which transmits information from the memory cartridge to the tally database, but stated that the voting system event logs would not record any of the possible malfunctions, "making it impossible to provide a more definitive answer."[152]

Nine days after the September primary, the D.C. Council subpoenaed information about the voting machines' source code from Sequoia so that it could conduct a more thorough investigation.[153] According to the *Washington Post*, Sequoia objected to this request on the grounds that it constituted trade secrets or otherwise protected material.[154] The vendor also objected to the Council's request for all documents related to any irregularities in similar voting systems, stating that *it had no documentation of such incidents.*[155]

The *Post* reported that when the Council persisted in its attempts to get the information, the company asked for a $20 million bond to guarantee confidentiality.[156] According to board officials, the company still had not responded to the subpoena as of late April 2009.[157] In April, the Council filed a motion in the District of Columbia Superior Court to attempt to force the company to comply with the subpoena.[158] On June 5, under a protective order from a Superior Court Judge, Sequoia agreed to release the source code for the voting system.[159] When news of the agreement broke, Councilwoman Mary Cheh said, "they fought us tooth and nail until now."[160]

"AS IT IS NOW, THERE'S LITTLE COMMUNICATION BETWEEN JURISDICTIONS, SO VENDORS HOLD ALL THE CARDS." DISTRICT OF COLUMBIA COUNCILMEMBER MARY CHEH

The findings of the District of Columbia investigation will soon be made public. In the interim, the Council passed election reform legislation that includes a 'warranty provision' requiring any vendor that sells voting systems to the District to "[p]romptly and fully disclose any flaw, defect, or vulnerability in the voting system of which the vendor is aware or becomes aware" and to remedy the problem appropriately.[161]

While this bill will help D.C. election officials get needed information about voting system defects in the future, Councilmember Mary Cheh still sees a need for a centralized, national database. "It was difficult for us to get the information we needed in D.C. If we were in a smaller, more fragmented, or politically divided jurisdiction, it would have been even harder for us to get necessary information in an expeditious fashion," said Cheh. "As it is now, there's little communication between jurisdictions, so vendors hold all the cards."[162]

• • •

13. New Jersey, February 2008

According to a public records request for results obtained by researchers at Princeton University, thirty-eight Sequoia AVC Advantage DRE voting machines in eight New Jersey counties experienced anomalies during the February 5, 2008 primary election.[163] A county official initially discovered the problem by comparing machine counter totals with the paper printouts produced by the machines at the close of the polls.[164] The county alerted other counties, which do not routinely reconcile these two totals, to the potential malfunction.[165] The *Times of Trenton* reported that the problem initially appeared

to be with the turnout totals – while all votes seemed to be correctly recorded, the total number of individuals who cast votes for each party appeared to be slightly off.[166] Sequoia inspected the equipment and concluded that the problem was poll worker error, not equipment malfunction.[167] In early March, the company issued a technical bulletin advising users of the machine on how to protect against this error in the future.[168]

In March, several counties decided to enlist a team of Princeton computer scientists to conduct an independent study on the equipment used in the February primary. After the counties' intent to hand over their voting machines for assessment became known, one of the researchers who was set to conduct the analysis reported on his blog that he received an e-mail from Sequoia stating that the company will "take appropriate steps to protect against any publication of Sequoia software, its behavior, reports regarding the same, or any other infringement of [its] intellectual property."[169] The *Star-Ledger* reported that at least one county which subsequently backed the effort received a letter from Sequoia stating that conducting an independent investigation would violate the licensing agreement between the vendor and the county, and threatening to sue if the county proceeded with the inquiry.[170] In addition, that same month, advocates at the Rutgers Constitutional Litigation Clinic issued a subpoena for the necessary information to conduct an independent analysis, including the machines' source code, build tools, operator manuals, and maintenance manuals.[171] According to the Princeton researchers' final report, Sequoia "vigorously protested" sharing its source code on grounds of defending its intellectual property and it took "months of litigation" to negotiate a protective order under which Sequoia would share the information.[172] In May, a Superior Court judge issued a protective order permitting the team of Princeton researchers to examine two of the DREs used in the February primary but preventing the disclosure of "any conclusions or comments" about the machines resulting from the investigation.[173]

OFFICIALS IN MONTGOMERY COUNTY, PENNSYLVANIA, AN AVC ADVANTAGE COUNTY LOCATED LESS THAN FIFTY MILES FROM THE NEW JERSEY BORDER, TOLD THE PHILADELPHIA INQUIRER THAT THEY WERE UNAWARE OF THE PROBLEMS THAT HAD OCCURRED IN NEW JERSEY.

In June, after the plaintiffs who issued the subpoena and researchers conducting the assessment refused to sign the protective order on the grounds that it violated their speech rights and academic freedom, the judge who issued the initial protective order reversed her ruling with respect to the non-disclosure of the researchers' findings.[174] The results of the released independent analysis showed the researchers concluded that on all but one of the thirty-eight machines that malfunctioned during the primary, the number of votes for candidates of a certain party exceeded the number of individuals who voted on that party's ballot.[175] Some machines logged more votes for Democrats than Democratic voters, and others logged more votes for Republicans than the number of Republican voters.[176] The researchers concluded that it would be "easy and natural" for poll workers to make the mistake that triggered the programming error that produced incorrect vote totals. Some voters were effectively disenfranchised by this error. Those who received the wrong party's ballot could not choose a candidate of their own party as was their legal right, and write-in votes for their chosen party were not counted because it is unlawful for a voter to vote in the primary election of a party to which she does not belong.[177] Furthermore, the researchers identified serious insecurities in the machines, and stated that the machines could be quickly and imperceptibly hacked to steal votes by anyone with "only ordinary training" in computer science.[178]

Had advocates and researchers in New Jersey not been persistent in their efforts to overcome Sequoia's resistance to a thorough and independent investigation of its machines, these flaws may never have come to light. Indeed, even given the significant media attention that the incident received, other users of AVC Advantage machines were unaware of the malfunctions that occurred in New Jersey. In March of 2008, after county election officials in New Jersey had begun clamoring for an investigation of the machines' behavior in the February primary, officials in Montgomery County, Pennsylvania, an AVC Advantage county located less than fifty miles from the New Jersey border, told the *Philadelphia Inquirer* that they were unaware of the problems that had occurred New Jersey.[179] Were Sequoia obligated to report any known flaws in its voting system to a federal oversight agency, these problems may have been revealed more expeditiously.

• • •

14. Indiana, May 2006

Less than two weeks before the May 2006 primary election, voting machine manufacturer MicroVote admitted to election officials that the voting equipment it had sold to dozens of Indiana counties was uncertified, in violation of state law.[180] The delay in obtaining certification caused a panic amongst county election officials who faced the threat of legal action by the state if they used uncertified equipment in the primary.[181]

According to testimony and reports in the local media, while MicroVote continued to work toward certification, on April 22, ten days before the primary, it learned from the independent testing authority contracted to complete its certification that the company's voting machines would allow some voters to cast votes for candidates who would not represent them. The testing authority found that the company's Infinity DREs, installed in 47 counties across the state, allowed voters casting straight-ticket ballots in "split precincts," where voters living in the same precincts choose from different sets of candidates, to vote for the wrong set of candidates.[182]

In order to pass the certification process in time for the May 2 primary election, MicroVote opted to shut down the machines' straight ticket functionality altogether, allegedly at the advice of the independent testing lab.[183]

According to the *Indianapolis Star*, MicroVote worked in secret to develop a software update that would resolve the problem before the general election, when the straight-ticket function would be necessary in several split precincts.[184] A sales representative for the company testified that MicroVote installed the update on all Infinity DREs in the state without notifying the Indiana Election Commission, applying for certification only after the installation was complete.[185] Election officials only learned of the problem with the straight-ticket function when MicroVote applied for certification of this update, nearly four months after the company first became aware of the defect.[186]

Fortunately, the straight ticket function is not necessary in primary elections, but Indiana Election Code requires that certified equipment be functional for both primary and general elections.[187] Perhaps more importantly in the minds of Indiana election officials, MicroVote appeared to have concealed information from the Indiana Election Commission for months, and it is unclear what the company would have done had they failed to come up with a solution before the general election.[188] Upon learning of the glitch and of MicroVote's prior knowledge of the problem, Indiana Election Commission chair Tom Wheeler said he was "disturbed by [the company's] lack of candor."[189] One year later, an administrative law judge fined MicroVote over $360,000 for 198 violations of state election law occurring between October 2005 and the 2006 general election.[190]

THE SUBOPTIMAL STRUCTURE OF THE VOTING SYSTEM MARKET

Discussion of the need for regulatory reform in the voting system market is incomplete without mention of the market's suboptimal structure. Purchasing a particular voting system essentially binds election officials to the vendor who sold them their system for many years to come. Because officials have extremely limited funds, they are unlikely to turn to a new vendor when problems arise: the systems (from precinct voting machines to tally servers) are designed for matched components, which makes it impractical for officials to replace parts with those produced by a different vendor. Instead, they are effectively forced to buy an entirely new system and new machines for every polling place (an exceptionally expensive proposition). In addition to this cost, election officials bear the additional burden of training election workers, poll workers and educating the public on the new systems.

At the same time, as a result of contractual constraints and because voting system vendors generally have monopolies over the production of all replacement parts and exclusive control over the firmware and software in each system, election officials will generally remain extremely dependent upon the voting system vendor to address problems and ensure that their systems are working smoothly. This includes programming their machines, providing them with software patches, diagnosing and fixing malfunctions, and providing replacements when systems fail.

Vendors often constrain election officials in more explicit ways. Many contracts explicitly disclaim liability for damages resulting from problems that cause "data loss."[191] Furthermore, vendors have in the past threatened to sue election officials and others who publicize machine flaws or independently investigate and test machines malfunctioning machines.[192]

Election officials say this encourages them to keep quiet about machine malfunctions. Though understandable, this reluctance to publicize malfunctions contributes to the possibility that election officials and watchdog groups remain in the dark about known problems. Consequently, it is essential to provide election officials with protections against vendor retaliation. One solution is to allow election officials to post information about known problems on a nationwide database "semi-confidentially," meaning that only other election officials and/or the agency charged with maintaining the database could view the official's contact information. Similarly, through statute, Congress or the states could provide monetary penalties and perhaps the creation of a private right of action against vendors that retaliate and/or harass individuals or localities who report problems.[193] Last year's announcement that the largest voting system vendors, Election Systems and Software (ES&S) and Premier (formerly known as Diebold), planned to merge raised concerns. A central worry was that the merger would leave election officials in an even weaker position

relative to voting system vendors. At the time, the *New York Times* estimated that the merger would "mean that nearly 70 percent of the nation's precincts would use machines made by a single company."[194] The newspaper noted that this "would make it harder for jurisdictions to bargain effectively on price and quality" for new purchases.[195] More to the point, it would make jurisdictions more dependent on a single vendor – for everything from repairs to future service – and thus less likely to speak publicly about voting system deficiencies.

After the U.S. Department of Justice and nine state attorneys general filed an antitrust suit over the merger in March of 2010, the Department of Justice announced that it had secured an agreement from ES&S to divest itself of many of Premier's voting system assets (though not necessarily its service contracts).[196] In May, Dominion Voting Systems – another manufacturer with a significant share of the U.S. market – announced that it had acquired the assets of Premier from ES&S in accordance with the Department of Justice's proposed settlement.[197]

The merger highlights two major concerns for election officials in a market that just one vendor could eventually dominate. First, election officials' already weak leverage with vendors would further diminish, for if there is essentially just one vendor, there is no viable alternative vendor available, regardless of how poor the service or function of the machines.

Second, and perhaps more importantly as relates to this report, having the vast majority of the nation's voting systems manufactured and/or serviced by a single company could also mean much greater vulnerability nationwide to software bugs or other problems, particularly if such problems are not immediately publicly reported and corrected throughout the country.[198]

IV. A BETTER WAY TO TRACK AND ADDRESS VOTING SYSTEM PROBLEMS

As this report shows, the current regulatory scheme for voting systems does not adequately ensure that problems with these systems are detected and corrected.[199] The Brennan Center proposes a new regulatory structure to address this inadequacy, one based upon our interviews with election officials and regulatory experts, our review of analogous regulatory structures in other important industries. The new regulations and/or statute must include at least four key provisions:

1. **A Publicly Available, Searchable Centralized Database:** Election officials, in particular, would benefit from a publicly available, searchable online database that includes official (i.e., election official-reported or vendor-reported) and unofficial (i.e., voter-reported) data regarding voting system failures and vulnerabilities, and other reported problems and establishes criteria for the database's contents and organization.

2. **Vendor Reporting Requirements:** Vendors must be required to report to the appropriate government agency via the database and certified mail "early warning" data regarding known and suspected voting system failures and vulnerabilities, and other reported problems, including when vendors receive a complaint from a customer (an election official), when they receive a warranty claim and/or take some action to satisfy a warranty, when they conduct an investigation of a reported problem, and when a customer or other person sues them.

3. **A Federal Agency with Investigatory Powers:** The best way to ensure that vendors address potential problems in a timely manner is to empower the appropriate government agency to investigate all voting system failures and vulnerabilities listed on the database, grant the agency subpoena power to facilitate its investigations, and require vendors to, among other things, maintain records that may help the agency determine whether there are indeed voting system failures or vulnerabilities, and whether the vendor has taken appropriate action to address the failures or vulnerabilities.

4. **Enforcement Mechanisms:** The appropriate government agency must have the power to levy civil penalties on vendors who fail to meet the reporting requirement or to remedy failures or vulnerabilities with their voting systems.[200]

This section discusses in detail how we believe each of these critical provisions should be drafted, analogous legislation and regulations that contain similar provisions, and the key benefits that the new provisions would bring to the regulation of voting systems.

Of course, as with any regulation or law, good definitions will be critical to creating an effective regulatory scheme. We provide suggested definitions for many key terms used in these sections ("voting systems," "vendors" "failures," etc.) in Appendix A.

1. A Publicly Available, Searchable Centralized Database

A robust regulatory system should mandate the creation of a searchable online database. It should be easily accessible through the appropriate government agency's home page. And, it should contain comprehensive information about all reported voting system failures, usability concerns, vulnerabilities,

or potential vulnerabilities by any person, including, among others, machine vendors, election officials, and voters. Vendor reporting of such problems should be mandatory. Reporting from others should be permissive. Additionally, while voters, election officials, and others should be able to simply upload their reports to the database via the Internet (*subject to review by the appropriate agency*), vendors would be required to both upload the reports to the database via the Internet and send the reports to the appropriate government agency via certified mail.

As already discussed (*supra* p. 25), given their ongoing reliance on voting system vendors to repair and service their systems, election officials should have the option of filing reports confidentially, meaning they can request no individuals except other election officials know their identity. This would encourage more honest and timely reporting by those most likely to observe voting system malfunctions.

A SEARCHABLE, CENTRAL DATABASE COULD "SERVE AS A REPOSITORY TO LET ME KNOW WHAT ISSUES EXIST WITH THE MACHINE, RATHER THAN HAVING TO RELY ON WHAT THE VENDORS SPOON-FEED ME."
ROKEY SULEMAN, EXECUTIVE DIRECTOR OF THE DISTRICT OF COLUMBIA'S BOARD OF ELECTIONS AND ETHICS

Similarly, it makes sense to provide whistleblowers working for voting machine companies and/or state and local governments with the option of requesting that personal information be kept confidential. To ensure confidentiality, Congress would probably have to provide a FOIA exemption for reports filed by election officials.[201]

A searchable database would have benefits beyond the issuance of "advisories" to customers upon a problem's discovery. In part because of high turnover among election officials, such advisories can get lost from election to election (*see, e.g.,* the Humboldt County, California case study discussed *supra* pp. 12 - 13). Moreover, officials looking to purchase or deploy new systems will not necessarily have easy access to advisories issued by a vendor or the EAC (in the case of EAC certified systems) in the recent or distant past. By making it simple for election officials and the public to search for problems and workarounds associated with voting systems at any time, a well designed database could increase the likelihood that jurisdictions looking to use new machines would learn about potential problems *before* purchase or use.

A. Provision Details

A bill or new regulations addressing this issue should set specific requirements for reports, including: (1) a description of the make and model of the voting machine involved;[202] (2) the jurisdiction(s) in which the machine is being used, if applicable; (3) a description of the nature of the problem or concern with the machine; (4) the date of the discovery of the problem or concern; (5) the name and contact information for the person submitting the report; (6) a verification by the person submitting the report that the information submitted is true and accurate and that the person consents to such information being included in the database; (7) versions of hardware, software, and firmware affected; and (8) any suggested workarounds and fixes, or instructions for how to retrieve this information when it becomes available.

Regulations should stipulate that the database be searchable by: (1) the date of discovery of the problem with the voting machine; (2) the make and model of the voting machine involved; (3) the nature of the problem with the machine; (4) the jurisdiction in which a system is used; and (5) such other categories as the appropriate government agency deems necessary. Additionally, we propose that the legislation or regulatory framework include a provision that prohibits the appropriate government agency from disclosing to anyone other than an election official the contact information of an election official, voter, or vendor employee who submits a report to the database without the express written consent of the person submitting this information.[203]

The database should also be searchable by and distinguish among reports submitted by (1) election officials, acting in their official capacities on behalf of their governmental units; (2) vendors; and (3) all other submitters, including voters, whistleblowers and anyone else. Voters, election officials, and vendors are likely to discover very different issues with voting systems, and their reports are likely to carry different weights with different audiences. This division should particularly help election officials, voting rights groups, and any agency investigating potential problems.

Finally, the agency responsible for creating and maintaining the database should probably be given some ability and responsibility to review reports before they are posted, to ensure that on their face they belong on the database. Allowing anyone to report anything without a filter could allow individuals to overload the database with useless or irrelevant reports, resulting in an essentially useless database.[204]

B. Responsible Agency

The EAC could construct and maintain the database. The EAC is already in the business of establishing "voluntary" guidelines to which new voting systems are tested. Section 202 of HAVA gives the EAC the responsibility of serving as a "national clearinghouse and resource for the compilation and review of information" related to the administration of elections. And, as already discussed (*supra* pp. 8 - 9) the agency collects anomaly reports provided by vendors and election officials for the few systems it has certified. The EAC does not currently list the data it receives from vendors and election officials in the kind of searchable database that other agencies use, and that we believe would be most useful to election officials, but there is no reason it could not do so in the future (in fact, this may be largely addressed with the adoption of a new clearinghouse policy in the near future).

More problematically, the EAC has taken the position that its powers to facilitate the understanding and resolution of problems with non-EAC certified voting equipment is extremely limited, absent explicit Congressional authority that does not currently exist.[205] As the vast majority of machines currently in use in the United States have not been certified by the EAC,[206] this could represent a serious impediment to the creation of a database under the auspices of the EAC, absent a clarification from the EAC or Congress. As the Government Accountability Office has noted, if Congress explicitly expands the EAC's powers in this regard, it should also consider providing the EAC with the additional resources necessary to take on this additional work.[207] The EAC's Voting System Testing and Certification Program currently employs only five staff members.[208]

Alternatively, the Comptroller General and the GAO could assume responsibility for the database. The GAO has a strong reputation of competence and impartiality, and it has a well-established track record for acquiring and publicizing information.[209] It has also already done a considerable amount of work related to HAVA and voting machines,[210] and has in fact noted the void that currently exists in identifying and resolving problems with non-EAC-certified voting systems, in particular.[211]

Finally, the Department of Justice could create and maintain the database. The Department has similar responsibilities in other contexts. For instance, the Anti-Car Theft Improvements Act of 1996[212] gave the DOJ responsibility for creating the National Motor Vehicle Title Information System, a database designed to compile information from a variety of sources on the histories of individual motor vehicles. The Act also provided the Department with enforcement powers in the event someone required to submit information to the database failed to do so.

C. Analogous Regimes

Analogous regulatory regimes for other industries demonstrate the power and usefulness of this kind of regulatory scheme.

The clearinghouse we propose is similar in principle to the database that Congress ordered the Consumer Product Safety Commission (CPSC) to establish as part of the Consumer Product Safety Improvement Act (CPSIA) of 2008.[213] One of CPSIA's key features was Congress's mandate that the CPSC create a publicly available, searchable database that records information from, among others, consumers, government agencies, and healthcare professionals, regarding the harms related to the use of a consumer product regulated by the CPSC.[214] A House Committee Report on the legislation states that the "goal of the CPSC should be to devise a database that can rapidly provide consumers with 'early warning' information about specific products that could pose serious safety hazards."[215]

The National Highway Traffic Safety Administration (NHTSA)[216] and the Food and Drug Administration (FDA) maintain similar "early warning" databases. NHTSA's Early Warning Reporting database collects and makes publicly available property damage reports and death and injury reports provided by manufacturers pursuant to the Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act of 2000.[217] Meanwhile, NHTSA's Office of Defects Investigations (ODI) database, even before the passage of the TREAD Act, has allowed consumers both to make and search for safety complaints regarding problems with motor vehicles or pieces of motor vehicle equipment.[218] The FDA's Adverse Event Reporting System, moreover, collects and makes publicly available adverse drug reaction information by healthcare professionals and consumers.[219]

These databases, although not quite as robust and user-friendly as the proposed CPSIA database, have played important roles in protecting the public. Indeed, it was independent analysis of NHSTA's complaint database that catalyzed the Bridgestone/Firestone tire recall years ago.[220] And, it was the Bridgestone/Firestone recall that was the impetus behind the passage of TREAD.[221]

In June 2009, researchers mining the NHTSA complaint database discovered the high rate of failure of Chinese valve stems; this ultimately led to the recall of millions of valve stems in vehicle tires.[222] Later in the year, NHTSA launched an investigation of Toyota vehicles after receiving over 400 consumer complaints about acceleration problems with the cars; some of these problems appear to have been responsible for fatal accidents.[223] This investigation led Toyota to announce on November 25 that it would repair the accelerator pedals on some 4.26 million vehicles.[224] After the first recall, reports of problems with Toyota vehicles, which had been steady before acceleration problems began to receive attention in the fall, surged.[225] As more customers came forward with complaints, federal investigators expanded the probe to look at other problems with Toyota vehicles, and the company issued additional recalls for brake and acceleration problems.[226] On April 5, 2010, NHTSA assessed the largest legally permissible fine against Toyota. In his letter to the company notifying them of the fine, NHTSA Chief Counsel O. Kevin Vincent identified the manufacturer's failure to notify authorities in a timely manner after becoming aware of the defects as the primary rationale for levying the harsh penalty.[227]

Results from the FDA's Adverse Event Reporting System have been no less powerful. For example, in 1998 shortly after the System's launch, reports of liver injuries on the system resulted in the FDA's removal of the anti-inflammatory drug Duract from the market.[228] More recently, a handful of reports on the system about a serious condition affecting bone marrow of those taking the antibiotic Zyvox, led to a change to the drug's labeling to inform providers about the risk of this reaction and recommendations for monitoring patients. [229] We chose the CPSIA database as a model because it will be the most comprehensive publicly available "early warning" database ever created, and the CPSC has been developing it based upon lessons from the NHTSA and FDA databases with a desire to improve upon them by, among other things, making them more user-friendly.[230] Indeed, in CPSIA's legislative history, a House Committee urges the CPSC to "examine these and other Agency efforts, if applicable, when designing its own database."[231]

D. Key Benefits

A database that conforms to the specifications we have outlined would allow the appropriate government agency, vendors, and the public to efficiently access, evaluate, investigate, and share information regarding voting system failures or vulnerabilities. This, in turn, would result in earlier detection of system failures and vulnerabilities by vendors and election officials, and ensure more rapid responses to those issues ultimately making it less likely that voting systems will malfunction on Election Day, when it matters most. More specifically, however, the database would achieve the following objectives:

Increase Election Official & Public Awareness of Problems & Solutions

A NATIONAL, SEARCHABLE DATABASE WOULD ALLOW ELECTION OFFICIALS TO EASILY ACCESS AND SHARE INFORMATION.

The database would allow election officials to easily access and share information. For example, this would help to ensure that election officials in different states using the same make and model of machine or other voting system element would be aware of any problems the other had encountered using that equipment – if one official discovers a vulnerability and posts this information to the database, the other official will be able to check his or her system to ensure that it does not also have that vulnerability. Moreover, if a vendor provides one election official with a procedural solution, such as a workaround to address a problem, the database would provide officials using the same voting equipment in other jurisdictions with that solution.

Further, the database would provide voter protection groups, political parties and other concerned members of the public with more knowledge about potential voting system problems. Before an election, they would, among other things, be able to determine whether there have been any issues with the voting systems in their counties and, if so, to advocate corrective action before the election and be on the lookout for similar problems during voting.

Improve the Ability of Government and Others to Identify Failures or Vulnerabilities & Respond Quickly

The database would allow the appropriate government agency, voter protection groups, and other concerned members of the public to mine the information on the database and spot patterns and trends that may indicate voting system failures or vulnerabilities. This is a key reason for allowing individual voters to report problems they encounter. All of the databases hosted by federal agencies that we reviewed allow such reporting from the general public. After collecting and analyzing this information, the appropriate government agency would be able to more quickly launch an investigation to rectify these potential vulnerabilities or failures.

Provide Timely & Organized Access to Information

The database would include all of the reports uploaded to it in an easily searchable format essentially in real time. It would help to eliminate the thousands of state and county government silos by centralizing all the data in one place. Further, placing the database on the Internet via a single home page would significantly increase the accessibility of the information to all.

Assist Election Officials in Evaluating the Comparative Performance of Voting Systems

By allowing for searches by the make and model of a voting machine or other voting system component among other datasets, the database would provide election officials with a helpful resource to determine which equipment has been the most reliable. This information would be particularly useful for election officials considering the purchase of new voting systems.

Provide Election Officials and Others with the Opportunity to Identify Machine Issues without Fear of Retribution

A provision that prohibits the government from disclosing the contact information of any election official or other person who submits a report to the database to persons other than election officials without the written consent of that person protects the confidentiality of these individuals; this protection reduces the risk that a voting system vendor attempts to harass or seek retribution against them for posting a negative report to the database. For similar reasons, there should be monetary penalties and perhaps the creation of a private right of action against vendors that retaliate and/or harass individuals or localities, including especially whistleblowers, who report problems.

2. Vendor Reporting Requirements

A. Provision Details

New legislation or regulations should require voting system vendors to provide "early warning" data to the appropriate government agency regarding voting system failures or vulnerabilities. This would go well beyond what manufacturers of the few EAC certified systems must currently report to the EAC (see *supra* pp. 8 - 9) if they wish to maintain that EAC certification. We propose that the government require *all* vendors to provide written notification via certified mail (in addition to uploading the information to the database) when they determine that a voting system failure or vulnerability may exist, including when

- they receive a complaint from a customer (an election official);
- they receive a warranty claim and/or take some action to satisfy a warranty;
- they conduct an investigation of a reported problem; and
- a customer or other individual sues them.

The legislation or regulations should set specific requirements for the notification, including: (1) the location of the failure or vulnerability; (2) a description of the failure or vulnerability; (3) the vendor of the voting machine; (4) the jurisdictions where the machine is used; (5) an evaluation of the risk to election outcomes related to the failure or vulnerability; (6) the vendor's intended remedy for it; (7) versions of hardware, software, and firmware affected; and (8) any suggested workarounds and fixes, or instructions for how to retrieve this information when it becomes available. It is critical that the EAC

or other relevant federal agency has the discretion to require vendors to include other information in the notice, and to require further reporting related to any corrective action plan, to ensure that (when necessary) remedial steps are taken and are adequate.

B. Responsible Agency

Just as the EAC, GAO or DOJ would be appropriate agencies to appoint to create and maintain the database, all three would be appropriate agencies to vest the power to require vendors to provide additional information in the required notice. Whichever agency is assigned responsibility for maintaining the database and setting notice requirements for vendors should also probably be the agency which receives such notices.

C. Analogous Regimes

The same federal agencies that maintain the databases discussed above: NHTSA, the CPSC, and the FDA, also require manufacturers to report "early warning" and other data directly to them. Our proposed reporting requirements for voting machine vendors are similar to these regimes, particularly in respect to the contents of the required notices.

There are two types of requirements for reporting problems to NHTSA: reports regarding "early warning" data and reports regarding defects. Regarding "early warning data," rules promulgated by the Secretary of Transportation[232] under the authority of the TREAD Act[233] require manufacturers to submit information on each make and model of vehicle offered for sale in the United States within the previous two years that details (1) incidents involving death or injury that were alleged or proven to be caused by a possible defect, including foreign incidents occurring in substantially similar or identical vehicles; (2) property damage claims, warranty claims, and consumer complaints; and (3) field reports identifying defects, fires, or rollovers.[234] Requirements for other types of vehicles and equipment such as child restraints and tires are substantially similar.[235] After submitting a one-time report of historical information covered by the regulations,[236] manufacturers must submit the information described above on a quarterly basis.[237]

If a manufacturer identifies a defect[238] and determines "in good faith" that the defect has an impact on motor vehicle safety or that the vehicle or equipment does not comply with applicable safety standards, the manufacturer must notify the Secretary of Transportation and all owners, purchasers, and dealers of the vehicle or equipment in question.[239] This notification must contain: (1) a clear description of the defect or noncompliance; (2) an evaluation of the risk associated with the defect; (3) the measures to be taken to obtain a remedy; (4) a statement that the manufacturer will provide the remedy without charge; (5) the period during which the defect will be remedied without charge; and (6) the procedure for notifying the Secretary of Transportation of the manufacturer's failure to remedy a defect as mandated by law.[240] Depending on the magnitude of the risk presented by the defect and the cost of providing public notice relative to number of additional owners the notice is likely to reach, the Secretary of Transportation may also require manufacturers to provide public notice.[241]

Reporting requirements to the CPSC are similar to those for NHTSA. Manufacturers who discover that a product does not comply with product safety rules or standards or contains a defect that creates the risk of injury or death are required to inform the CPSC of the problem.[242] If the CPSC determines that the noncompliance or defect constitutes a substantial product hazard requiring consumer notification,

the CPSC may compel the manufacturer to stop distribution; notify those involved in the transport, distribution, or sale of the product by mail or other means; provide public notice on the Internet, TV, and radio; and/or mail notice to all known purchasers of the product.[243]

The CPSC has the authority to determine the form and substance of any such notice,[244] but the law provides some guidelines for manufacturers. Unless the CPSC rules otherwise, all notices must contain, among other things, (1) identifying information such as a model number and photograph of the product; (2) a description of the action taken to remedy the defect or noncompliance; (3) a description of the hazard caused by the product; (4) a number and description of injuries and deaths caused by the product; (5) a description of available remedies and how to avail oneself of them; and (6) retail information concerning the product.[245]

MANDATORY VENDOR REPORTING OF FAILURES TO A SEARCHABLE DATABASE WOULD INCENTIVIZE THOSE VENDORS TO ENHANCE INTERNAL CONTROLS.

Finally, the FDA requires all manufacturers of all drugs marketed under an approved FDA application to report to the FDA all serious, unexpected adverse drug experiences associated with the use of their drug products.[246] The FDA mandates that the manufacturer submit to it, within fifteen days of learning of the adverse drug experience, a form[247] that contains: (1) a description (i.e., sex, age, weight, height) of the patient that took the drug; (2) the outcomes attributed to the adverse event; (3) the date of the event; (4) the date of the report; (5) a description of the event; and (6) various information regarding the product suspected to be the cause of the event.[248]

D. Key Benefits

Many of the benefits of mandatory vendor reporting of machine failures and vulnerabilities are the same as those of the proposed database (e.g., assisting election officials in identifying and resolving problems, aggregating information in a timely and organized manner, and allowing election officials to compare the performance of voting systems); below we detail some additional benefits that are particular to the proposed vendor reporting requirements.

Incentivizes Vendors to Enhance Internal Controls

Vendors will presumably want to minimize the number of reports that they must make to the appropriate government agency. One way that they will be able to do this is by enhancing their own testing and internal standards to avoid any late-stage defects that would trigger a requirement to make a report to the appropriate government agency.

Ensures Maximum Disclosure of Information by Vendors

As we detail above, Congress passed the TREAD Act and established these "early warning" reporting requirements, in part, because investigations in the wake of the Firestone tire recall revealed that "both Firestone and Ford knew that there were problems [with the tires] years before they told [NHTSA] or the American public."[249] The case studies in Part III of this report show that, at the very least, many election officials and other concerned citizens worry that voting system vendors have sometimes taken too long to acknowledge and publicize problems with their systems. This provision would require vendors to take

affirmative steps to increase their transparency and would ensure, among other things, that at the very least, election officials and the appropriate government agency will have access to problems soon after vendors discover them.

3. A Federal Agency with Investigatory Powers

A. Provision Details

If this new regulatory structure is going to be effective, a federal agency must have adequate enforcement authority. The most logical model would allow the appropriate federal agency to initiate an investigation after reviewing any of the information posted to the database and determining that a machine failure or vulnerability potentially exists.

In order to facilitate these investigations, new legislation should provide the appropriate federal agency with the power to issue subpoenas and include a provision that would require vendors of electronic voting machines to maintain records, reports, and other information to enable the agency to determine whether there is compliance with other provisions of the legislation.

B. Responsible Agency

The EAC already has some investigatory powers related to its federal certification program. Specifically, manufacturers who register to have new voting systems federally certified by the EAC must, pursuant to the EAC's VSTCPM (discussed previously at page 8),[250] agree to "[c]ooperate with any EAC inquiries and investigations into a certified system's compliance with VVSG standards and the procedural requirements of this Manual . . . ."[251] While the VSTCPM does not currently require vendors to report all of the types of problems we have detailed (*see supra* pp. 8 - 9) to a centralized database (none currently exists, of course), we could imagine an amendment to the VSTCPM which would require such reporting as part of the Voting System Testing and Certification Program, and require manufacturers to cooperate with any investigations into their compliance with such mandates. Of course, as previously noted in this report, the EAC is currently limited to investigating manufacturers registered under the Voting System Testing and Certification Program, and who stay registered under that program.[252] For this reason, Congress might need to explicitly empower the EAC to employ these investigatory powers as applied to problems arising with non-EAC certified systems. It would also probably need to provide the EAC with extra funding, as the EAC has previously stated that even if given this power, it does not have the resources to track and resolve problems related to non-EAC certified systems.[253]

Alternatively, the GAO regularly conducts investigations in support of its mission.[254] As discussed in greater detail below, the GAO is almost certainly constitutionally barred from taking enforcement action against vendors or others, but as a legislative agency, it should have the power to investigate and gather information.[255] Consequently, if the GAO is given responsibility for creating and maintaining the database, it might well make sense to also give it explicit investigatory powers necessary to ensure that the database is accurate.

Finally, it may make sense to vest investigatory powers with the Department of Justice, an agency with a substantial infrastructure to conduct investigations and bring enforcement actions, where necessary.[256] The Voting Rights Section of the Civil Rights Division at the Department of Justice has a long history of taking enforcement actions under a variety of federal laws relating to voting, including voting machines, and also has experience administering complex statutory schemes.[257] The

Civil Division of the Department of Justice has experience enforcing an even wider variety of federal laws and regulations; the Federal Programs Branch of the Civil Division assists federal agencies like the Department of Energy, Housing and Urban Development, the Department of Health and Human Services, and others to carry out their regulatory obligations by initiating litigation against those who violate statutes or regulations.[258] In fact, giving the Department of Justice investigatory and enforcement powers would be consistent with the structure that already exists in HAVA. While HAVA assigns the EAC a clearinghouse and advisory role, it also gives the DOJ enforcement authority to bring an action for declaratory and injunctive relief for failure to comply with HAVA's minimum requirements for voting systems, provisional voting and voter registration.[259]

C. Analogous Regimes

Both NHTSA and the CPSC have broad investigatory powers.[260] The CPSC has the authority to enter and inspect any factory, establishment, or conveyance used to facilitate placing goods into the stream of commerce.[261] NHTSA has similar authority.[262] The simple ability to investigate information uploaded to their databases, of course, falls within the ambit of these agencies' powers. For example, it is the responsibility of the Office of Defects Investigations within NHTSA to "elicit from every available source and evaluate on a continuing basis any information suggesting the existence of a safety-related defect."[263] NHTSA's databases allow the ODI to both elicit and evaluate this information, and as we have discussed above,[264] investigations initiated after reviewing information in the databases have been fruitful.

Both NHTSA and the CPSC have subpoena power[265] and a recordkeeping requirement for the entities that they regulate.[266] We propose that the new provision closely track this language, particularly that of the Consumer Product Safety Act of 1972.[267]

D. Key Benefits

Ensures Reliability of Information on the Database

The information posted to the proposed database must be accurate so that false information does not mislead election officials, the public, the government, EAC, or unfairly sully vendors' reputations. The government will need the tools necessary to ensure that only accurate information is posted to and remains on the site.

Grants the Government Power to Effectively Respond to Information it Receives

A recordkeeping requirement would allow the appropriate government agency to address reported failures or vulnerabilities of the machines quickly, without having to wait for vendors to gather this information. Moreover, granting subpoena power to the appropriate government agency ensures, among other things, that the agency will be able to gather the information it needs to adequately judge the seriousness of reported problems and ensure that proper steps have been taken to prevent malfunctions or other failures from happening in the future.

4. Enforcement Mechanisms

A. Provision Details

New legislation or regulations should give the appropriate agency adequate enforcement powers by authorizing it to seek civil penalties against voting system vendors for failure to comply with their duty to report any voting system failure or vulnerability or to remedy the issue after learning about it. It should also cap the penalty amount for a series of related violations at a specific dollar amount; similarly, there should be a specific dollar cap on the penalty amount for problems for any individual model and version of a product.

B. Responsible Agency

As already discussed, the Department of Justice and the Voting Rights Section of its Civil Right Division have a long history of taking enforcement actions under a variety of federal laws related to voting. In fact, according the Department's website, it has filed a dozen actions to enforce various HAVA requirements, including requirements related to voting machines.[268] Accordingly, the most logical place to house enforcement powers related to the database is with the Department.

HAVA already divides authority between the EAC and DOJ, giving the EAC responsibility for providing information and advising local jurisdictions, and giving the Department of Justice enforcement powers.

ENSURING THAT THE APPROPRIATE FEDERAL AGENCY CAN ENFORCE NEW VENDOR REPORTING REQUIREMENTS WOULD HELP RESTORE PUBLIC CONFIDENCE IN VOTING SYSTEMS.

The EAC's ability to take enforcement actions against manufacturers is likely to be more limited. As already discussed, the EAC currently has the power to decertify systems[269] it previously certified (which is only a small percentage of systems currently used in the United States)[270] or suspend the registration of a manufacturer[271] seeking federal certification for new systems for various infractions. This does not include failure to report to a central database, but we can imagine an amendment to the VSTCMP that allows the EAC to take such actions for failure to comply with database reporting requirements. However, using decertification and/or suspension of registration would be rather blunt instruments for what could, in many cases be relatively minor infractions. As the VSTCPM itself notes, "[d]ecertification is a serious matter. Its use will significantly affect Manufacturers, State and local governments, the public, and the administration of elections."[272] It is doubtful that the EAC would want to take such a drastic step for all but the most serious infractions. At the same time, the EAC does not have the power to decertify systems it has not certified, which represents the vast majority of the systems in use today.[273]

While it may be technically possible for the EAC to take additional enforcement action – such as seeking imposition of monetary penalties – if Congress amended HAVA to vest it with that power – it is not clear that the agency currently has the infrastructure or institutional knowledge to carry out such tasks. the GAO is almost certainly constitutionally barred from taking any enforcement action, as it is considered a creature of Congress, which prevents it from taking actions that amount to executing the law.[274]

C. Analogous Regimes

Civil penalty provisions are not uncommon in analogous regulatory regimes. Recently the trend has been for Congress to increase such penalties. For example, in 2002, the TREAD Act increased the penalties originally established in the Vehicle Safety Act of 1966[275] that NHTSA could seek to have imposed on vehicle manufactures from $1,000 per violation to $5,000 per violation and from a penalty cap of $800,000 to a cap of $15,000,000.[276] Similarly, in 2008, CPSIA dramatically increased the civil penalties already provided for in the Consumer Product Safety Act of 1972 (e.g., from $5,000 per violation to $100,000 per violation) for knowing sale of products that do not conform to an applicable rule or standard or failure to make necessary records available to the CPSC.[277] The penalty language legislation should resemble the language of both the Vehicle Safety Act and the Consumer Product Safety Act.

D. Key Benefits

Increases Vendor Accountability

As Part III (*Failures of the Current System: Case Studies*) of this report illustrates, in the past, vendors have not been held accountable for voting machine failures or their inability or refusal to correct them. Legislation with enforcement mechanisms would provide the EAC or another federal agency with the necessary enforcement tools to hold vendors accountable for their acts or omissions after an investigation and hearing shows that this is justified.

Incentivizes Vendors to Quickly Comply with Mandates

Civil penalty provisions would act as a deterrent to wrongdoing by vendors; penalties would be high enough so as to not simply be regarded by vendors as a cost of doing business.

Helps to Restore Public Confidence in Voting Systems

HAVA was meant to help restore public confidence in the integrity of the electoral process. During the signing ceremony for HAVA, President Bush stated that "[t]he legislation I sign today will add to the nation's confidence."[278] He further added, "[t]hrough these reforms, the federal government will help state and local officials to conduct elections that have the confidence of all Americans."[279]

Giving an independent government agency the power to investigate problems and take action to remedy problems should greatly increase public trust in our voting systems and elections.

WHAT LOCAL GOVERNMENTS CAN DO NOW

While a national, centralized and searchable database along the lines we have suggested in this report is ultimately the best way to ensure that problems with machines are publicized and corrected throughout the country, there are important interim steps that county and state governments, in particular, can begin taking immediately to increase the chances that election officials learn of problems with their voting systems and can avoid some of the kinds of problems detailed in this report

Negotiate Better Contracts

As previously detailed in this report, provisions in many voting machine contracts make it much more difficult for election officials and the public to get detailed information about system problems reported in other parts of the country, or to hold vendors responsible for problems when something goes wrong. To increase voting system reliability and maximize vendors' motivation to minimize the risk of such problems, counties and states should begin demanding certain key contract terms, including:

- mandating reports from vendors "on a per occurrence basis of any hardware or software system error occurrences resulting from design or manufacturing defects in any jurisdiction" in which the voting system is being used;[280]
- mandating reports from vendors of any complaints (including usability concerns), warranty claims and lawsuits about their systems, together with the result of any vendor investigation, explanations, and actions taken to address these complaints;
- extending warranty periods for the purchasers;
- mandating financial liability to vendors in the event of a malfunction;
- ensuring that voting systems are tested against the most modern federal guidelines instead of older versions that computer scientists have faulted as inadequate; and
- allowing local election officials to independently test the accuracy of the machines as long as they do not disclose proprietary information or trade secrets.[281]

The New Jersey Department of the Public Advocate discusses how jurisdictions might construct many of these provisions in a document entitled "The Purchase of Voting Systems in New Jersey: How Government Can Better Protect Taxpayer Rights and Voting Security."[282] Washington, D.C. has also passed a law setting more stringent requirements for voting system contracts.[283] We strongly urge election officials entering into contracts with voting system vendors to review the contents of these documents.

Of course, adding these kinds of provisions to contracts will probably only be of benefit to jurisdictions as they negotiate *new* contracts. Jurisdictions not purchasing new voting systems in the near future (i.e., the vast majority of counties and states throughout the country) are unlikely to secure agreement from vendors to substantially amend their contracts along these lines.

Furthermore, even if all jurisdictions were able to get these kinds of provisions into their contracts, it would still be important to mandate many of these provisions in regulation. For instance, if a vendor violates the notification terms of its contract with a small county in Arkansas by failing to inform it of a voting system malfunction in New Jersey, the Arkansas County is unlikely to find out about the violation under current circumstances. More to the point, even if it does learn of such a failure, the county is unlikely to bring an action under the contract (for all of the reasons discussed on pages 25 - 26 of this report) unless the malfunction brings disastrous results in its own election sometime later. The point of the database and stronger regulation is to minimize the likelihood of such occurrences by bringing problems to light *before* they can cause such significant harm.

Implement Stronger State Regulation

The legislature in at least one state, California, has passed legislation requiring vendors selling systems within its borders to notify the Secretary of State and all local election officials using its systems of any "defect, fault or failure" it discovered, within 30 days of discovery.[284] As of the writing of this report, the legislation awaits a decision by the governor, who vetoed an earlier version of the bill in 2009.[285] This bill would empower the Secretary of State to seek monetary penalties against vendors for failing to comply with reporting requirements, and requires the Secretary to notify the EAC of the problem.

While the California proposal would not have solved all of the problems identified in this report, it would have gone a long way toward forcing vendors to begin to publicly report problems with their systems when alerted to them. It could also have provided many of the benefits (albeit on a smaller scale) that a national centralized database would provide: in particular, increasing vendor accountability and incentivizing vendors to enhance internal controls; benefiting state certification programs by supplying tips for targeted testing and review of the effectiveness of mitigations proposed by vendors; allowing election officials (in California, anyway) to get up-to-date information about their systems before deploying them in elections.

The California model presents the best legislative attempt we have seen, to date, to address the problems we have discussed in this report. We hope the governor will sign this bill into law and that other states will follow suit.

Still, the limitations of this proposal as compared to a *national* clearinghouse are obvious. Among other things, the California bill only requires reporting for systems used in

California; the bill does not mandate a searchable database that new election officials could review before each election; and because the bill could not provide a method for election officials and whistleblowers to anonymously report problems that might not technically fall within the definition of "defect, fault or failure" (such as the problems in Pulaski County, Arkansas, described on page 14 of this report), it would not necessarily result in the sharing of information about some kinds of problems that still result in the loss of hundreds and thousands of votes.

Create a Voluntary Database

While the EAC has previously indicated that it does not believe it has the authority or resources to facilitate the understanding and resolution of problems with non-EAC certified voting equipment, we can think of no legal reason why – even absent additional authorization from Congress – it could not create a searchable database to which election officials, voters, and vendors could report. In the alternative, if the EAC determines it does not have the resources to create such a database, election officials, through organizations such as the National Association of Secretary of States, the National Association of State Election Directors, , the National Association of County Recorders, Election Officials and Clerks, or the International Association of Clerks, Recorders, Election Officials and Treasurers could sponsor such a database. There would be no way to force vendors to report to this database, or to provide election officials with whistleblower protections for making voluntary reports – two important suggestions for the mandatory clearinghouse detailed in this report – but it could still lead to a much better resource for election officials than currently exists. Election officials using the same equipment could also create user groups where they could share information about their systems electronically.

Officials we interviewed wanted to see a database that vendors would be required to report to, but many said they viewed a voluntary database as a good first step. For instance, Cuyahoga County, Ohio Board of Elections Director Jane Platten stated that "an exchange of all information about anomalies, malfunctions and failures of voting systems is not only much needed, but should be a requirement." However, she added that "taking the small step of creating a voluntary exchange of information would in my opinion have a huge impact on election administration and operations."

Pressure Vendors to Voluntarily Post Information on Their Own Sites This Year

One drawback of the three previous recommendations – in addition to the larger recommendation of the creation of a central, mandatory, and federal database – is that each will take time to implement, and probably cannot be accomplished in time for this fall's election. By contrast, vendors could significantly reduce the risk of a repetition of past problems with their systems by creating their own databases, and offering election officials who use their machines access to them. As already noted in this report, because there is such high turnover among election officials, a new county director might not be aware of product advisories or software patches sent by a voting system vendor to her predecessor three years earlier. Nor is she likely

to be aware of problems reported by election officials in other counties. Those problems could have been caused by poll worker error, a misuse or misprograming of the system, or a host of other reasons that are not related to a software or hardware malfunction – but that could still easily be repeated in other counties in future elections.

Ideally, vendors would create for election officials a central, easily accessible and searchable site where they could review all previously issued product advisories, software patches and workarounds, and a list of all election official complaints, warranty claims and lawsuits about their systems (together with the result of any vendor investigation, explanations, and actions taken to address these complaints). This would provide election officials with an opportunity to be more fully appraised of potential problems and safeguards that could be taken ahead of each election.

County and state officials can and should demand this voluntary action from vendors now, in time to make a difference for November's election and reduce the likelihood that we will see a repetition of previous system failures.

Ultimately, of course, a mandatory reporting system with clear guidelines will be preferable. As Butler County, Ohio Board of Elections Director Betty McGary put it, "[C]learly when a vendor is continuing to sell their product in a State, they are not going to be excited about *voluntarily* reporting deficiencies in their systems . . . requiring the reporting be mandatory will be the only way" to get comprehensive cooperation.

V. CONCLUSION

Voting is the most important of all our federal rights. It is the right that protects all other rights. Despite this, we have all too often been strangely cavalier about protecting it. The very different way we regulate voting systems and other commercial products clearly dramatizes this fact.

Given the billions of dollars spent by federal and local government to purchase and maintain new voting systems over the last decade,[286] the failure to take stronger measures to ensure that we are tracking and correcting system failures is particularly troubling.

We propose a regulatory scheme that would greatly improve our election systems. It would:

- help level the playing field between election officials and vendors as they negotiate over service and hardware contracts;
- increase vendor accountability and incentivize vendors to enhance internal controls;
- provide public advocacy and voting rights groups with data on potential problems with voting systems;
- provide the government and concerned citizens with the ability to locate patterns of problems;
- benefit state certification programs by supplying tips for targeted testing and review of the effectiveness of mitigations proposed by vendors;[287] and perhaps most importantly,
- allow election officials to get the most up-to-date information about their systems before deploying them in elections.

In light of the importance of safeguarding our democracy through accurate and fair elections, these are especially worthwhile goals. We encourage policymakers to work with regulatory experts in other fields, consult database experts, and talk to election officials and voting system vendors to ensure the creation and quick use of the best and most effective database possible.

APPENDIX A : IMPORTANT DEFINITIONS

As with any new statute or regulation, defining key terms will be critical to the effective implementation of the proposals in this report. Among other things, a new statute or regulation must clearly define (1) what kind of equipment is covered; (2) what types of problems *must* be reported; and (3) *who* must report such problems.

What equipment should be covered by this new regulatory scheme?

Voting Systems: the new statute should cover "voting systems" as defined in Section 301(b) of the Help America Vote Act,[288] and in addition should include electronic poll books.

Electronic Poll Books: electronic poll books are used with increasing frequency around the country.[289] As with voting machines, electronic poll books rely on software and firmware that can be subject to bugs, misprogramming and other glitches. And as with voting machines, electronic poll book malfunctions have caused long lines, and the likely disenfranchisement of many voters.[290] For this reason, we believe electronic poll books should be covered under a new regulatory scheme. Such poll books might be defined as "an electronic mechanism (including stand-alone software) by which an election official at a polling place, at the time an individual seeks to vote, may obtain information on the individual's eligibility to vote (including whether the individual is registered to vote in an election for Federal office, the polling place to which the individual is assigned, and whether the individual has already voted in the election), whether the mechanism is operated by integration with a voting system or independently."

What types of problems must be reported?

To reduce the kinds of problems that cause lost votes, voting system vendors should be required to report both voting system failures *and vulnerabilities* they have knowledge of. In the course of testing, servicing and repairing machines, vendors may become aware of vulnerabilities that have yet to cause a system failure, but that could be reasonably expected to cause a failure in the future. Vendors should also be required to make reports to the database when they receive a complaint from a customer (i.e., election official), whether or not they agree that their machine was the cause of the alleged problem; when they receive a warranty claim and/or take some action to satisfy a warranty; when they are notified by a customer of a usability issue that could lead voters or poll workers to operated the system in a way that would lead to disenfranchisement or the recording of an unintended vote; when they conduct an investigation of a reported problem; and when a customer or other person sues them.

System Failures[291]: The term "system failure" should mean any event that results in

(a) loss of one or more voting system functions;
(b) degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds;
(c) automatic reset, restart or reboot of the voting device, operating system or application software;
(d) a requirement for an unanticipated intervention by a person in the role of poll worker or technician before the test or operation of the device can continue;
(e) error messages and/or audit log entries indicating that a failure has occurred; or
(f) failure to tabulate, tally, or report results accurately.

System Vulnerabilities: should include any flaw in a voting system which might reasonably lead to a System Failure.

Who must report problems?

Anyone, including election officials, should be permitted to report voting system problems. For the reasons detailed in this report, if the new regulatory scheme is going to have maximum effectiveness, voting system vendors must be *required* to report both failures and vulnerabilities brought to their attention.

Voting System Vendor should include any sole proprietor, partnership, LLC, corporation, commercial entity or non-commercial entity that has contributed to the initial development, building, distribution or other parts of the supply chain, or maintenance of all or part of the voting system.

Who is entitled to ask that their personal information be kept confidential?

At the very least, election officials and whistleblowers who work for vendors or state and local governments, should be entitled to request that their name and identifying information be kept confidential.

A provision establishing this confidentiality option might look like this:

> (a) If information is submitted for inclusion in [the database] by or on behalf of an election official who affirmatively requests that his name and identifying information be kept confidential, [the agency] shall not release to the public the submitters' name and identifying information, notwithstanding the provisions of Title 5 United States Code Section 552 or other provision of law, unless the [head of agency] determines that such public disclosure is necessary to advance the purposes of this chapter.
>
> (b) In the case of information submitted for inclusion in [the database] by or on behalf of any person other than an election official or a voting machine vendor, [the agency] shall not release to the public the submitters' name and identifying information, notwithstanding the provisions of Title 5 United States Code Section 552 or other provision of law, unless the submitter affirmatively authorizes such release or the [head of agency] determines that such public disclosure is necessary to advance the purposes of this chapter.
>
> (c) Except as provided in subsections (a) and (b) of this section, [the agency] shall make all information submitted for inclusion in [the database] available to the public.

APPENDIX C : DuPAGE COUNTY ELECTION SUMMARY*

DuPage County Election Summary
General Primary Election – March 16, 2004

May 18, 2004

Introduction

This document outlines the areas of DuPage election support that I was personally involved with where I believe there is room for improvement. Some of these ideas were generated by discussions at the DuPage post-election meeting and others from my own evaluation of the processes that I observed during the recent election.

Suggestions for Improvement

Pre-election planning – In order to properly plan for all the tasks and deadlines that are involved with an election in DuPage, we need to develop a formal project plan and project schedule. These planning devices will help ensure that important tasks are not overlooked, and that critical dates and deadlines are recorded and shared between the DuPage Election Commission staff and Fidlar.

Suggestions:

DELETED

GEMS Upload Failure on York 58 – This memory card had a failed upload transmission on election night that was not detected until the next day when reports were run on the precinct, and zero results were found for each race within the precinct. The status of the memory card upload within GEMS was "successful" but the upload record showed the ballot count to be zero. It is rather discomforting that this failed transmission was not detected on election night.

*Sections of this document have been deleted by the Brennan Center to include only those paragraphs relevant to this report. A complete copy of the document is on file with the Brennan Center.

ENDNOTES

1. Definitions for key terms such as 'voting systems' used in the report can be found in Appendix A.

2. Telephone Interview with Denise Lamb, Chief Deputy Clerk for Elections, Santa Fe County, New Mexico (Sept. 30, 2009).

3. United States Election Assistance Commission, *Election Administration and Voting Survey Frequently Asked Questi*ons, http://www.eac.gov/research/election_administration_and_voting_survey_faqs.aspx (last visited Aug. 9, 2010); Spencer Overton, *Stealing Democracy*, http://www.stealingdemocracy.com/facts.cfm (last visited Aug. 9, 2010).

4. The Proposed Final Judgment and Competitive Impact Statement are reprinted in 75 Fed. Reg. 12256-12270 (Mar. 15, 2010).

5. S.B. 1404, 2009-10 Reg. Sess. (Cal. 2010).

6. Specifically, S.B. 223 2005-06 Reg. Sess. (N.C. 2005) states that "[t]he vendor shall promptly notify the State Board of Elections and the county board of elections of any county using its voting system of any decertification of the same system in any state, of any defect in the same system known to have occurred anywhere, and of any relevant defect known to have occurred in similar systems."

7. *See* Michael Traugott, et. al., The Impact of Voting Systems on Residual Votes, Incomplete Ballots, and Other Measures of Voting Behavior (conference paper presented at the Midwest Political Science Association, Chicago, IL, Apr. 7-10, 2005), Charles Stewart III, *Residual Vote in the 2004 Election* (Caltech/MIT Voting Technology Project, VTP Working Paper No. 2.3, 2005).

8. 42 U.S.C. §§ 15322, 15371(a) (2009).

9. 42 U.S.C. § 15322 (2009).

10. Sarah F. Liebschutz and Daniel J. Palazzolo, *HAVA and the States*, 35 Publius: J. of Federalism 497 (2005), *available at* http://publius.oxfordjournals.org/cgi/reprint/35/4/497.pdf; Press Release, Representative Rush Holt, Holt Urges Election Assistance Commission to Address Voting Machine Failures, Accessibility in 2010 Election Survey (Nov. 19, 2009), *available at* http://www.house.gov/apps/list/press/nj12_holt/111909.html; VotersUnite!, Proposal to the EAC: A Public Information-Exchange Mechanism Regarding Fielded Voting Systems (May 2008), *available at* http://www.votersunite.org/info/EACInfoClearinghouseProposal.pdf.

11. E-mail from Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (Sept. 10, 2010, 15:01 EST) (on file with the Brennan Center).

12. Testimony of Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission, *available at* http://www.eac.gov/News/docs/04-08-10-eac-public-mtg-testimony-layson-final.pdf/attachment_download/file.

13. Testimony of Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission, *available at* http://www.eac.gov/assets/1/AssetManager/05-27-10%20EAC%20Public%20Mtg%20Testimony%20Layson%20FINAL.pdf.

14. E-mail from Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (May 19, 2010, 13:58 EST) (on file with the Brennan Center).

15. United States Government Accountability Office, Report to the Chairman, Committee on House Administration, House of Representatives: Federal Program for Certifying Voting Systems Needs to Be Further Defined, Fully Implemented, and Expanded 4-5, 31 (September 2008), *available at* http://www.gao.gov/new.items/d08814.pdf?source-ra [hereinafter *GAO Voting Systems Report*]. ("The scope of EAC's efforts to track

and resolve problems with certified voting systems does not extend to those systems that were either qualified by NASED or were not endorsed by any national authority. According to program officials, the commission does not have the authority or the resources needed to undertake such a responsibility … As a result, the commission's efforts to track and resolve problems with voting systems do not include most of the voting systems that will be used in the 2008 elections.").

16. United States Election Assistance Commission, Testing and Certification Program Manual Version 1.0 (2007) [hereinafter VSTCPM].

17. E-mail from Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (May 14, 2010, 17:09 EST) (on file with the Brennan Center).

18. *Id.*

19. VSTCPM, *supra* note 14 at 2.3.2.7.

20. Telephone Interview with Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission (Aug. 25, 2010).

21. VSTCPM, *supra* note 14 at 8.7.3.

22. United States Election Assistance Commission, Voting System Testing and Certification Program Voting Systems Technical Advisory Intermittent Freeze/Shutdowns with EAC Certified ES&S Unity 3.2.0.0 System (2010), http://www.eac.gov/assets/1/AssetManager/Product_Advisory-ES&S-06.25.10%20FINAL.pdf.

23. *Id.*

24. United States Election Assistance Commission, Voting System Testing and Certification Program Voting System Technical Advisory Configuration Management Issues with EAC certified MicroVote EMS 4.0B (Modification) (2010), http://www.eac.gov/assets/1/AssetManager/MicroVoteEMS40B_Product_Advisory-final_august_23_2010.pdf.

25. E-mail from Matt Masterson Deputy Director of the EAC's Testing and Certification Program to Lawrence Norden, Senior Counsel, Brennan Center for Justice (July 1, 2010, 11:20 EST and Aug. 26, 2010, 15:32 EST) (on file with the Brennan Center) (Confirming that two counties in Ohio, two counties and twenty-two towns, cities, and villages in Wisconsin, twenty-two counties in Florida, and nine counties in Iowa, use certified equipment); E-mail from Matt Masterson Deputy Director of the EAC's Testing and Certification Program to Lawrence Norden, Senior Counsel, Brennan Center for Justice (Aug 31, 2010, 11:16 EST) (on file with the Brennan Center) (Confirming that Delaware uses EAC certified central count machines to count absentee ballots. Its polling place machines are not EAC certified).

26. Counties may "upgrade" existing systems to versions that will be EAC certified. But for the most part, given the current economic climate, counties and states around the country are unlikely to receive big grants to purchase entirely new equipment.

27. United States Election Assistance Commission, State Requirements and the Federal Voting System Testing and Certification Program, 5 (2009), http://www.eac.gov/assets/1/Page/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf.

28. VSTCPM, *supra* note 14 at 8.7.4.

29. Letter from Douglas A. Kellner, Co-Chair of the New York State Board of Elections to the Honorable Thomas R. Wilkey, Director of the EAC (June 30, 2010).

30. *Compare* County of San Diego Registrar of Voters Contract No. 46619 between County of San Diego and Diebold Election Systems, Inc. and Diebold Incorporated at 20-21 (2003), *available at* http://accurate-voting.org/contracts/CA/San_Diego/CA_sandiego_2003.pdf (demonstrating an contractual obligation for the county to inform the vendor of defects in the voting system with no similar obligation on the part of the vendor), *with* Contract No. 08455, Voting Equipment Agreement between Election Systems and Software, Inc. and Kansas Secretary of State at 7 (Nov. 16, 2005) (stating that the contractor will notify the customer of any defects or problems that arise).

31. E-mail from Jane Platten, Director, Cuyahoga County Board of Elections, to Lawrence Norden, May 27, 2010.

32. For examples of a lag in vendor acknowledgement of voting system problems, see the case studies in this report from Butler County, Ohio (at pp. 10 - 11) and Humboldt County, California (at pp. 12 - 13).

33. By usability concerns we mean flaws in the machine's programming, software or hardware that make poll worker or voter error significantly more likely, and which lead to significant disenfranchisement.

34. This appears to be precisely what occurred in Humboldt County, California in 2008. This case is detailed on pages 12 - 13.

35. E-mail from Betty McGary, Executive Director, Butler County Board of Elections, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (May 17, 2010 11:58 EST) (on file with the Brennan Center); *see also* Letter from Betty McGary, Executive Director, and Lynn Kinkaid, Deputy Director, Butler County Board of Elections, to Dave Byrd, President, Premier Election Solutions (Apr. 4, 2008) (on file with the Brennan Center) [hereinafter *McGary Letter 1*].

36. Lynn Hulsey, *Voting Machine Maker Says Error May Cause Votes to be Uncounted*, Dayton Daily News, Aug. 23, 2008, at A6.

37. Editorial, *That's a Pretty Big Glitch*, N.Y. Times, Oct. 9, 2008, at 36. The paper refers to the manufacturer in this incident as Diebold.

38. McGary Letter 1, *supra* note 30.

39. Letter from Betty McGary, Executive Director, and Lynn Kinkaid, Deputy Director, Butler County Board of Elections, to Dave Byrd, President, Premier Election Solutions (Apr. 9, 2008) (on file with the Brennan Center).

40. *See* Premier Election Solutions, Review of Butler County March 2008 Primary Election Issues (May 2008).

41. E-mail from Betty McGary to Lawrence Norden, *supra* note 30.

42. Office of the Ohio Sec'y of State, Premier Memo (Aug. 21, 2008) (on file with the Brennan Center).

43. *Id.*

44. *Id.*; Letter from Dave Byrd, President, Premier Election Solutions, to Jennifer Brunner, Ohio Sec'y of State (Aug. 19, 2008) (on file with the Brennan Center).

45. *Id.*

46. E-mail from Betty McGary to Lawrence Norden, *supra* note 30.

47. Telephone Interview with Carolyn Crnich, Registrar of Voters, Humboldt County, California (Sept. 29, 2009) [hereinafter *Crnich Interview*].

48. Thaddeus Greenson, *Software Glitch Yields Inaccurate Election Results*, The Times-Standard, Dec. 12, 2008, http://www.times-standard.com/localnews/ci_11145349; Kim Zetter, *Serious Error in Diebold Voting Software Caused Lost Ballots in California County*, Threat Level (Blog of Wired Magazine), Dec. 8, 2008, http://www.wired.com/threatlevel/2008/12/unique-election [hereinafter *Zetter 2008*].

49. E-mail from Carolyn Crnich, Clerk, Humboldt County, California, to Lawrence Norden, Senior Counsel, Brennan Center for Justice at New York University School of Law (May 1, 2010, 12:00 EST) (on file with the Brennan Center).

50. *Id.*

51. Crnich Inteview, *supra* note 42.

52. Zetter 2008, *supra* note 43; Jaikumar Vijayan, *California Finds E-Voting Software Had Errors, Data Deletion Functions*, Computerworld, Mar. 4, 2009.

53. Debra Bowen, California Sec'y of State, Report to the Election Assistance Commission Concerning Errors and Deficiencies in Diebold/Premier GEMS Version 1.18.19 2, 4 (2009).

54. *Errors and Deficiencies in Diebold/Premier GEMS version 1.18.19, Hearing before California Secretary of State Panel* 19 (Mar. 17, 2009) (statement of Justin Bales, General Manager for Western States, Premier Elections Solutions) [hereinafter *Bales Testimony*].

55. Crnich Interview, *supra* note 42.

56. Bales Testimony, *supra* note 49, at 20.

57. Crnich Interview, *supra* note 42.

58. *See* Florida Division of Elections, Analysis and Report of Overvotes and Undervotes for the 2006 General Election, General Over Undervote Table, *available at* http://election.dos.state.fl.us/reports/index.shtml.

59. Mary K. Garber, Voting System Performance Problems – Conclusions and Recommendations, in *Assessing Election Accuracy in Florida's 2006 General Election: A Comparison of Voting System Performance Using Undervote Rates in Statewide Races in Florida's 2006 General Election* (Dec. 2008) (unpublished manuscript, on file with the Brennan Center) [hereinafter *Garber manuscript*].

60. *Id.*

61. *Id.*

62. Kim Zetter, *Lost E-Votes Could Flip Napa Race*, Wired, Mar. 15, 2004, *available at* http://www.wired.com/politics/security/news/2004/03/62655.

63. *Id.*

64. *Id.*

65. Garber manuscript, *supra* note 54.

66. *Id.*

67. E-mail from Mary K. "Kitty" Garber, Associate Director, Florida Fair Elections Center, to Lawrence Norden, Senior Counsel, Brennan Center for Justice at NYU School of Law (Apr. 12, 1010, 15:17 EST) (on file with the Brennan Center).

68. E-mail from Bill Cowles, Supervisor of Elections, Orange County, Florida, to Laura Seago, Research Associates, Brennan Center for Justice at NYU School of Law (May 5, 2010, 9:34 EST) (on file with the Brennan Center).

69. Lawrence Norden, et. al., Is America Ready to Vote? State Preparations for Voting Machine Problems in 2008 (Brennan Center 2008), *available at* http://www.brennancenter.org/content/resource/is_america_ready_to_vote [hereinafter *Is America Ready to Vote*].

70. Daniel Nasaw, *Voting Machine Claim to be Studied by County*, Arkansas Democrat-Gazette, May 20, 2006 [hereinafter *Nasaw*].

71. Nasaw, *supra* note 65; Height Could Make a Difference in this Year's Elections (THV Broadcast, May 20, 2006) (transcript available at http://www.todaysthv.com/news/news.aspx?storyid=28836) [hereinafter *THV*];

72. THV, *supra* note 66.

73. *See* Margaret McDowell, Cheryl Fryar, Cynthia Ogden, and Katherine Flagal, National Center for Health Statistics, National Health Statistics Reports No. 10, Anthropometric Reference Data for Children and Adults: United States, 2003–2006 16 (2008).

74. Nasaw, *supra* note 65.

75. *See, e.g.,* Sarah Everett, The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection (May 2007) (Unpublished PhD dissertation, Rice University) *available at* http://chil.rice.edu/research/pdf/EverettDissertation.pdf, Bryan Campbell and Michael Bryne, Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability (2009) (paper presented at 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections) *available at* http://www.usenix.org/event/evtwote09/tech/full_papers/campbell.pdf.

76. Nasaw, *supra* note 65.

77. *Id.*

78. M.C. Moewe, *Voting Machine Maker Admits Problem*, Daytona Beach News-Journal, Nov. 3, 2007, at 1A. In the article, the paper refers to the manufacturer as Diebold.

79. *Id.*

80. *Id.*

81. *Id*.

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*

88. M.C. Moewe, *Info on Voting Flaws Not Shared*, Daytona Beach News-Journal, Nov. 12, 2007, at 1A.

89. *Id.*

90. *Id.*

91. Jeremy Milarsky and Rafael A. Olmeda, *Software Tweak Restores Votes*, Sun-Sentinel, Nov. 5, 2005, at 23A.

92. Eliot Kleinberg, *Broward Machines Count Backward*, Palm Beach Post, Nov. 5, 2004, at 29A [hereinafter *Kleinberg*]; *see also* Mark Leon Goldberg, *Don't Count on It: Why We Need Paper Trails to Back Up Compromised and Fallible Voting Machines – and Why We're Not Getting Them*, The American Prospect, Jan. 2005, at A20.

93. Milarsky and Olmeda, *supra* note 86.

94. Milarsky and Olmeda, *supra* note 86, Kleinberg, *supra* note 87.

95. Kleinberg, *supra* note 87.

96. Mary Ellen Klas and Gary Fineout, *Touchscreen Voting Machines Have Software Flaw, Florida Officials Learn*, Miami Herald, Jun. 12, 2004, at 1B [hereinafter *Klas and Feinout*].

97. Mary Ellen Klas, *Flaw in Florida Touch-Screen Voting Machines Was Known in 2002*, Miami Herald, Jun. 12, 2004, at 1B.

98. Klas and Fineout, *supra* note 91.

99. *Id.*

100. *Id.*

101. Klas, *supra* note 92.

102. Helen Gao, *Faulty Switches Blamed for Voting Woes*, San Diego Union Tribune, Apr. 14, 2004, at B-3 [hereinafter *Gao*].

103. Luis Monteagudo Jr. and Helen Gao, *Glitches in Voting Machines Examined*, San Diego Union Tribune, Mar. 4, 2004, at B-1 [hereinafter *Monteagudo and Gao*].

104. *Id.*

105. *Id.*

106. Gao, *supra* note 97.

107. Bill Ainsworth, *Tech Says Diebold Knew of Problem*, San Diego Union-Tribune, Apr. 22, 2004, at B-1 [hereinafter *Ainsworth*]; Hearing Before the Cal. Sec'y of State Voting Systems and Procedures Panel (Apr. 21, 2004) (statement of James Dunn) [hereinafter *Dunn Testimony*]; *Touch-Screen Trouble*, ABC News, Oct. 27, 2004, *available at* http://abcnews.go.com/Politics/Vote2004/story?id=203866&page=1.

108. Dunn Testimony, *supra* note 102, at 73.

109. *Id.* at 77-78.

110. Ainsworth, *supra* note 102; Hearing Before the Cal. Sec'y of State Voting Systems and Procedures Panel (Apr. 21, 2004) (statement of Robert Urosevich) at 59.

111. Frank Zoretich, *Election Results Certified After Software Blamed*, Albuquerque Tribune, Nov. 19, 2002 (on file with the Brennan Center) [hereinafter *Zoretich*].

112. Dan McKay, *County Certifies Vote Tally*, Albuquerque Journal, Nov. 19, 2002, at D1; Zoretich, *supra* note 106.

113. Zoretich, *supra* note 106.

114. Dan McKay, *Voting Machines Criticized*, Albuquerque Journal, Sept. 26, 2004, at A1.

115. Supplemental Brief for the petitioner at 10 (citing James A. Noel Aff. ¶¶ 3-8) Lopategui v. Vigil-Giron ex. rel., No. CV 2005-0433 (N.M. 2d Dist. Ct. Dec. 20, 2005).

116. *Id.*

117. *Id.*

118. Zoretich, *supra* note 106.

119. Telephone Interview with Denise Lamb, Chief Deputy Clerk for Elections, Santa Fe County, New Mexico (Sept. 30, 2009).

120. Kim Zetter, *E-Vote Machines Drop More Ballots*, Wired, Feb. 9, 2004, *available at* http://www.wired.com/politics/security/news/2004/02/62206 [hereinafter *Zetter 2004*].

121. *Id.*

122. Telephone Interview with Cherie Poucher, Director, Wake County Board of Elections, in Raleigh, N.C. (Oct. 5, 2009) [hereinafter *Cherie Poucher interview*].

123. Zetter 2004, *supra* note 115.

124. *Id.*

125. Is America Ready to Vote, *supra* note 64.

126. Cherie Poucher interview, *supra* note 117.

127. Zetter 2004, *supra* note 115. According to Poucher, all but 78 recast their votes.

128. Zetter 2004, *supra* note 115.

129. 42 U.S.C. § 15481(a)(3)(A) (2010).

130. Noel Runyan, Collection of my Electronic Voting Experiences on the Sequoia Edge II (Verified Voting Foundation 2009), *available at* https://www.verifiedvotingfoundation.org/article.php?id=6717; *See, e.g.*, Noel Runyan and Jim Tobias, Accessibility Review Report for California, Top-to-Bottom Voting Systems Review (Office of the California Secretary of State 2007), *available at* http://www.sos.ca.gov/elections/voting_systems/ttbr/accessibility_review_report_california_ttb_absolute_final_version16.pdf.

131. Runyan, *supra* note 127.

132. *See, e.g.,* Runyan and Tobias, *supra* note 127.

133. In 2008 alone, there were 480 complaints characterized as "accessibility problems" logged on the Election Protection 866-OUR-VOTE system.

134. Cherie Poucher interview, *supra* note 117.

135. *Id.*

136. We suggest triggers for mandatory voter reporting at p. 32.

137. Julia O'Donoghue, *Big Questions about Voting Machines*, Reston Connection, Mar. 18, 2009, *available at* http://www.connectionnewspapers.com/article.asp?article=326929&paper=71&cat=104.

138. *See generally* Is America Ready to Vote, *supra* note 64.

139. Telephone Interview with July Flaig, Election Manager, Fairfax County, Virginia, Office of Elections (April 13, 2010).

140. *Id.*

141. *Id.*

142. *Id.*

143. Telephone Interview with Rokey Suleman, Executive Director, Washington, DC Board of Elections and Ethics (Apr. 1, 2010).

144. *Id.*

145. Mary M. Cheh, Phil Mendelson, and Harry Thomas, Council of the District of Columbia, Restoring Confidence in the District's Elections: Preliminary Report and Recommendations of the Council Board of Elections and Ethics Investigation Special Committee 1 (Oct. 8, 2008) [hereinafter *D.C. Council Report*].

146. *Id.*

147. Nikita Stewart and Elissa Silverman, *Primary Vote Still Doesn't Add Up*, Wash. Post, Sept. 22, 2008 at B1; Nikita Stewart, *District's Primary Results Certified*, Wash. Post, Sept. 26, 2008 at B1.

148. *Id.*

149. D.C. Council Report, *supra* note 140, at 4; Sequoia Voting Systems, Report to the District of Columbia Board of Elections and Ethics 1 (Sept. 22, 2008).

150. Sequoia Voting Systems, *supra* note 144.

151. *Id.* at 3 (emphasis added).

152. *Id.* at 1 (Sept. 22, 2008).

153. Committee Protective Order between Board of Elections and Ethics Investigation Special Committee of the District of Columbia Council and Sequoia Voting Systems, Inc. (Jun. 5, 2009), *available at* http://www.voteraction.org/files/Exhibit%20I%20-%20DC%20protective%20order.pdf [hereinafter *D.C. protective order*].

154. Nikita Stewart, *Cheh to Seek Court Order in Elections Code,* Wash. Post, Apr. 23, 2009.

155. Letter from Mary Ellen B. Offer to Mary M. Cheh, *Re: Subpoena Duces Tecum to Sequoia Voting Systems, Inc.*, (Sept. 26, 2008) ("[T]here are no documents that are responsive to this request with regard to the voting system used by the DCBOEE - a combination of the Eagle III-P precinct-based optical scan units, Edge I non-VVPAT touchscreen units and WinEDS 3.1.012.").

156. D.C. protective order, *supra* note 148; Tim Craig, *Firm to Give D.C. Information about Its Voting Devices*, Wash. Post, Jun. 6, 2009.

157. Stewart, *supra* note 149.

158. *Id.*

159. D.C. protective order, *supra* note 148; Craig, *supra* note 151.

160. D.C. protective order, *supra* note 148; Craig, *supra* note 151.

161. City Council R. 18A18-0238, 2009, Council Period 18 (D.C. 2009), 2009 D.C. Law L18-0103.

162. E-mail from David Zvenyach, Chief of Staff, Office of Councilmember Mary Cheh, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (Apr. 12, 2010, 18:17 EST) (on file with the Brennan Center).

163. Andrew W. Appel, et. al., Princeton University, Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine 117 (October 17, 2008) [hereinafter *Princeton Study*].

164. E-mail from Penny Venetis, Co-Director, Rutgers Constitutional Litigation Clinic, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (Apr. 8, 2010, 12:38 EST) (on file with the Brennan Center) [hereinafter *Venetis E-mail*].

165. *Id.*

166. Robert Stern, *Makers Defend Voting Booths; Tally Errors Blamed on Polling Workers*, Times of Trenton, Mar. 1, 2008, at A1.

167. *Id.*

168. Joe McIntyre, Senior Project/Account Manager, Sequoia, *WinEDS Technical Product Bulletin – AVC Advantage Party Turnout Issue/Operator Panel Usage* March 4, 2008.

169. Posting of Ed Felten to Freedom to Tinker, *Interesting E-mail from Sequoia*, http://freedom-to-tinker.com/blog/felten/interesting-email-sequoia (Mar. 17, 2008, 14:25 EST).

170. Carly Rothman, *Plan for Voting Machine Probe Dropped After Lawsuit Threat*, Star-Ledger, Mar. 18, 2008, *available at* http://www.nj.com/news/index.ssf/2008/03/voting_machine_maker_threatens.html.

171. Princeton study, *supra* note 158 at 113-114.

172. *Id.* at 1-2.

173. Joshua Brockman, *N.J. Voting Machines May Be Tested for Accuracy*, Nat'l Public Radio, http://www.npr.org/templates/story/story.php?storyId=90727541.

174. Venetis E-mail, *supra* note 159; Joe Ryan, *Judge Rules Public Can See Voting Machine Test Results*, Star-Ledger, Jun. 20, 2008, http://www.nj.com/news/index.ssf/2008/06/judge_lifts_gag_order_on_votin.html.

175. Princeton study, *supra* note 158 at 117-118.

176. *Id.* at 118.

177. Venetis E-mail, *supra* note 159.

178. Princeton study, *supra* note 158 at 8-10.

179. Derrick Nunnally, *Voter Interest Surges in Pennsylvania Suburbs*, Philadelphia Inquirer, Mar. 6, 2008, http://www.philly.com/philly/news/politics/suburban_pa/16327086.html?viewAll=y.

180. IC § 3-11-7.5-4(d); Rick Yencer, *Election Software Not Certified*, Star Press, Apr. 20, 2006, at 3A [hereinafter *Yencer 1*]; Cindy Larson, *Uncertified Voting Machines to Be Used*, News-Sentinel, Apr. 21, 2006 [hereinafter *Larson*]; Robert Annis, *Some Voting Results Questioned*, Indianapolis Star, Jan. 8, 2009, at 4Y [hereinafter *Annis*].

181. Yencer 1, *supra* note 175; Larson, *supra* note 175.

182. MicroVote General Corp, Admin Cause No. 06-003-ED (eResolution May 21, 2007), *www.in.gov/sos/elections/files/SOS_MicroVote_Order.pdf at 21* [hereinafter *Indiana administrative order*]; Rick Yencer, *Voting Machines to be Repaired*, Star Press, Sept. 26, 2006, at 3A [hereinafter *Yencer 2*].

183. Indiana Administrative order, *supra* note 177, at 21; Yencer 2, *supra* note 177; Jason Thomas, *Poll Machine Flaw Hidden, State Says*, Indianapolis Star, Sept. 25, 2006, at 1 [hereinafter *Thomas*].

184. Thomas, *supra* note 178.

185. Indiana administrative order, *supra* note 177, at 39.

186. *Id.* at 38.

187. *Id.* at 22.

188. *See* Thomas, *supra* note 178.

189. Thomas, *supra* note 178; Yencer 2, *supra* note 177.

190. Annis, *supra* note 175.

191. New Jersey Department of the Public Advocate, The Purchase of Voting Systems in New Jersey: How Government Can Better Protect Taxpayer Rights and Voting Security 3 (2009), *available at* http://www.state.nj.us/publicadvocate/public/pdf/The_Purchase_of_Voting_Systems_in_NJ_11-24-09.pdf [hereinafter New Jersey Public Advocate Report].

192. *Id*. at 5; Online Policy Group v. Diebold, 337 F. Supp. 2d 1195 (Cal. Dis. Ct. 2004); Cory Doctorow, *Sequoia Voting Systems Threatens Felten's Princeton Security Research Team,* Boinboing, Mar. 17, 2008, http://boingboing.net/2008/03/17/sequoia-voting-syste.html.

193. For a detailed discussion of how this kind of system could work, see pages 27 - 38 of this report.

194. Editorial, *The Voters Will Pay,* N.Y. Times, Feb. 25, 2010, at A26 [hereinafter *Voters Will Pay*].

195. *Id*.

196. Kim Zetter, *Feds Move to Break Voting-Machine Monopoly*, Wired, Mar. 8, 2010, *available at* http://www.wired.com/threatlevel/2010/03/ess-sued-in-antitrust-cas.

197. Press Release, Dominion Voting Systems, Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets from ES&S (May 19, 2010), *available at* http://www.dominionvoting.com/images/pdfs/DominionAcquiresPremierReleaseFinal4.pdf.

198. See Voters Will Pay, *supra* note 189.

199. *See* Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 15301–15545 (2008)).

200. ACCURATE, the multi-institution voting research center funded by the National Science Foundation (NSF), suggests a fifth provision that would greatly improve regulation of voting systems. Specifically, that "there should be a rich feedback loop – from problems to investigation to testing – that uses actual problems to inform future testing procedures." Deirdre Mulligan and Joseph Lorenzo Hall, Preliminary Analysis of E-Voting Problems Highlights Need for Heightened Standards and Testing, NRC Whitepaper 23 (2004). They note that current voting system guidelines "lack a process to incorporate suspected system failures or to address changing technology. In particular, [they] fail to establish standards that ensure performance data from the used to improve systems so that the same problems do not contaminate future elections. Problems need to be investigated, understood, and then fedback into the process of recertifying (at times recalling) existing systems and establishing the next set of [certification criteria]." Erica Brand, Cecilia Walsh, Joseph Lorenzo Hall and Deirdre K. Mulligan, Public Comment on the 2005 Voluntary Voting System Guidelines 30 (2005), *available at* http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf.

201. There is precedent for creation of such FOIA exemptions. The Homeland Security Act (6 USC § 133) granted an exemption for voluntarily submitted critical infrastructure information. Federal whistleblower protections similarly work to keep individuals who report problems from suffering reprisals. The Whistleblower Protection Act of 1989 states that the Special Counsel tasked with investigating allegations made under the act may not disclose the identity of the individual who filed the complaint without that person's consent except in cases where imminent danger to public health or safety makes such disclosure necessary. 5 U.S.C. § 1213(h). *See generally* 5 U.S.C. § 552(b)(3), which authorizes legislative carve-outs of FOIA, so long as such carve-outs are specific enough and leave no agency discretion.

202. For voters who may not know the specific make and model of the machine involved, a simple description of the type of machine will suffice as the EAC will be able to determine a machine's make and model from the other data submitted by the voter in the report.

203. New legislation should also authorize the relevant agency to seek penalties against voting machine vendors who take any retaliatory action against election officials who post to the site.

204. This type of screening occurs with similar reporting databases. For example, some states screen reports for inclusion in their highway accident databases. *See, e.g.*, Alaska Department of Transportation and Public Facilities, 2001 Alaska Traffic Accidents (May 2003), *available at* http://www.dot.state.ak.us/stwdplng/highwaydata/pub/accidents/2001aktraffix.pdf.

2005 See *GAO Voting Systems Report*, *supra* note 13 at 31; Email from Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission to Susan Greenhalgh, Spokeswoman, Voter Action, Sept. 22, 2008 (on file with the Brennan Center).

206. GAO Voting Systems Report, *supra* note 13 at 4-5.

207. *Id*. at 32-33.

208. E-mail from Jeannie Layson, Director of Communications and Congressional Affairs, U.S. Election Assistance Commission, to Lawrence Norden, Senior Counsel, Brennan Center for Justice (Sept. 10, 2010, 15:01 EST) (on file with the Brennan Center).

209. *See generally* Institute of Internal Auditors, The Government Accountability Office: Government Audit Standards and Institute of Internal Auditors: International professional Practices Framework: A Comparison; Frederick M. Kaiser, GAO: Government Accountability Office and General Accounting Office, CRS Report for Congress (Sept. 10, 2008) .

210. *See, e.g.*, Government Accountability Office, Election Reform: Nine States' Experiences Implementing Federal Requirements for Computerized Statewide Voter Registration Lists (Feb. 7, 2006); Government Accountability Office, Elections: Results of GAO's Testing of Voting Systems Used in Sarasota County in Florida's 13th Congressional District (Feb. 8, 2008); Government Accountability Office, Elections: States, Territories, and the District Are Taking a Range of Important Steps to Manage Their Varied Voting System Environments (Sept. 2008).

211. The GAO has asked Congress to consider expanding the EAC's role under HAVA to address this problem. GAO Voting Systems Report, *supra* note 13 at 34.

212. Pub L. 104-152, 49 U.S.C. §§ 30501-30505 (2010).

213. Consumer Product Safety Improvement Act, Pub. L. No. 110-314, 122 Stat. 3016 (2008) (codified in scattered sections of 15 U.S.C.).

214. *See* § 212, 122 Stat. at 3048–49 (codified at 15 U.S.C. § 2055a(a), (b)). There is currently a March 2011 deadline for implementation of the database, which is tentatively named Saferproducts.org. *See, e.g.*, *Consumer Product Safety Commission Oversight: Current Issues and a Vision for the Future: Hearing before the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection*, 111th Congress (2009) (statement of Inez Tenenbaum, Chairman, Consumer Product Safety Commission).

215. H.R. Rep. No. 110–501, at 43–44 (2007).

216. Congress created NHTSA in 1970. *See* Highway Safety Act, Pub. L. No. 91–605 § 201, 84 Stat. 1739 (1970).

217. *See* Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, Pub. L. No. 106–414, 114 Stat. 1800 (2000) (codified in scattered sections of 49 U.S.C.). Congress mandated that NHTSA conduct rulemaking to determine the manner and extent of the early warning data and its collection. § 3(b), 114 Stat. at

1801 ("[T]he Secretary shall initiate a rulemaking proceeding to establish early warning reporting requirements for manufacturers of motor vehicles and motor vehicle equipment to enhance the Secretary's ability to carry out the provisions of this chapter."). The regulations resulting from this mandate ultimately form the structure of the "early warning" database. *See, e.g.*, C.F.R. § 579.29 (a)(1) ("[E]ach report . . . must be submitted to NHTSA's early warning data repository identified on NHTSA's Internet homepage . . . . A manufacturer must use templates provided at the early warning website, also identified on NHTSA's homepage, for submitting reports.").

218. *See* Safercar.gov, http://www-odi.nhtsa.dot.gov/index.cfm (last visited May 28, 2010).

219. *See* Adverse Event Reporting System, http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Surveillance/AdverseDrugEffects/default.htm (last visited May 28, 2010).

220. *See, e.g.*, Keith Bradsher, *Firestone Engineers Offer a List of Causes for Faulty Tires*, N.Y. Times, Dec. 19, 2000, at C1.

221. *See, e.g.*, 146 Cong. Rec. 1778 (2000) (statement of Rep. Markey) ("This legislation was initially prompted by the Firestone recall of some over 6 million tires used primarily by the Ford Explorer.").

222 *See, e.g.*, David Shepardson, *Agency Ends Probe of Ford Tire Valves*, Detroit News, Apr. 30, 2009, at 6B.

223. *See, e.g.*, *Losing its Shine*, Economist, Dec. 12, 2009, at 76.

224. *Id.*

225. Alexandra Burzon, *Toyota Complaints Surged After First Recall*, Wall Street Journal, Mar. 11, 2010, at B7.

226. Posting of David Bailey and Chang-Ran Kim to Reuters.com, Toyota Faces New Probe on Corolla Steering, http://www.reuters.com/article/idUSTRE61D2TS20100217 (Feb 17, 2010, 18:56 EST).

227. Posting of Peter Valdez-Dapena to CNNMoney.com, NHTSA Seeks Maximum Fine Against Toyota, http://money.cnn.com/2010/04/05/autos/toyota_nhtsa_fine/index.htm?cnn=yes&hpt=Sbin (April 6, 2010, 14:01 EST)

228. *See, e.g.*, Editorial, *Caution Flags at the F.D.A.*, N.Y. Times, July 2, 1998, at A20.

229. *See* United States Food and Drug Administration, The Public's Stake in Adverse Event Reporting, http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Surveillance/AdverseDrugEffects/ucm179586.htm (last visited May 28, 2010).

230. For example, it is slightly onerous for a person to make a complaint on the NHTSA Complaint Reporting Form. It spans a minimum of six pages, and consumers are, among other things, asked to code portions of their complaints. *See* Defects & Recalls, File a Safety Complaint, http://www-odi.nhtsa.dot.gov/ivoq/index.cfm (last visited May 28, 2010).

231. H.R. Rep. No. 110–501, at 44 (2007).

232. The Secretary of Transportation has delegated this authority, among others, to NHTSA. *See* 49 C.F.R. § 1.50 (2009).

233. *See* 49 U.S.C. § 30166(m) (2008) ("[T]he Secretary shall initiate a rulemaking proceeding to establish early warning reporting requirements for manufacturers of motor vehicles and motor vehicle equipment to enhance the Secretary's ability to carry out the provisions of this chapter.").

234. 49 C.F.R. § 579.21(a)–(c) (2009).

235. 49 C.F.R. §§ 579.21–579.26.

236. 49 C.F.R. § 579.28(c).

237. 49 C.F.R. § 573.1(b)(3) (2009).

238. A defect is defined by law to mean "any defect in performance, construction, a component, or material of a motor vehicle or motor vehicle equipment." 49 U.S.C. § 30102(a)(2) (2008).

239. 49 U.S.C. § 30118(c). Manufacturers must send notification via first class mail to all registered owners of the vehicle or equipment in question. If the manufacturer is unable to notify the registered owner, it must notify the most recent known purchaser. 49 U.S.C. § 30119(d).

240. 49 U.S.C. § 30119(a)(1)-(6).

241. 49 U.S.C. § 30119(3).

242. 15 U.S.C. § 2064(b) (2008).

243. 15 U.S.C. § 2064(c)(1).

244. 15 U.S.C. § 2064(c)(1).

245. 15 U.S.C. § 2064(i)(2).

246. *See* 21 C.F.R. § 314.80, § 314.98 (2009). Moreover, due to the Dietary Supplement and Nonprescription Drug Consumer Protection Act of 2006, similar requirements also apply to OTC drugs that are marketed without an approved FDA application. *See* Dietary Supplement and Nonprescription Drug Consumer Protection Act, Pub. L. No. 109–462, 120 Stat. 3469 (2006) (codified as amended at 21 U.S.C. §§ 379aa–381 (2008)).

247. The Form is FDA Form 3500A. 21 C.F.R. 314.80(f) (2009).

248. *See, e.g.*, Medwatch, FDA Form 3500A, http://www.fda.gov/downloads/Safety/MedWatch/HowToReport/DownloadForms/UCM082728.pdf (last visited May 28, 2010).

249. 146 Cong. Rec. 1778 (2000) (statement of Rep. Markey). Similarly, Congress initially established the reporting requirements with the non-"early warning" defect in the Motor Vehicle and Schoolbus Safety Amendments of 1974. *See* Motor Vehicle and Schoolbus Safety Amendments, Pub. L. No. 93–492, 88 Stat. 1470 (1974) (codified as amended in scattered sections of 49 U.S.C.). Congress passed this legislation, in part, because some manufacturers refused to notify the public of defects; or, if the manufacturers acknowledged that there were defects, failed to timely notify consumers of them. *See, e.g.*, H.R. Rep. No. 93–1191, at 5 (1974).

250. VSTCPM, *supra* note 14.

251. VSTCPM, *supra* note 14 at 2.3.2.6.

252. That currently includes most manufacturers of voting systems used in the United States today. *See* United States Election Assistance Commission, Registered Manufacturers, http://www.eac.gov/voting%20systems/voting-system-certification/registered-manufacturers/ (last visited May 28, 2010).

253. GAO Voting Systems Report, *supra* note 13 at 31.

254. *See generally* Frederick M. Kaiser, *supra* note 203.

255. *See* Bowsher v. Merck & Co., 460 U.S. 824 (1983) (enforcing statutory requirement that government contractors provide data to the GAO).

256. See 42 U.S.C. § 1971(c).

257. United States v. New York State Board of Elections, *et. al,* 2006 U.S. Dist. LEXIS 27664 (N.D.N.Y 2006); 28 C.F.R. § 51 (2009).

258. *See* United States Department of Justice, Federal Programs Branch, http://www.justice.gov/civil/Federal%20Programs.htm (last visited May 28, 2010).

259. 42 U.S.C. § 15511 (2009).

260. *See* 49 U.S.C. § 30166 (2009); 15 U.S.C. § 2065(b) (2009).

261. 15 U.S.C. § 2065(a) (2009).

262. *See, e.g.*, 49 U.S.C. § 30166(b) (2009) ("The Secretary of Transportation may conduct an inspection or investigation that may be necessary to enforce this chapter.").

263. 49 C.F.R. § 554.5 (2009).

264. *See* Part IV.1.C, *supra*.

265. *See* 49 U.S.C. § 30166(g)(1)(B) (2009) ("[T]he Secretary . . . may conduct hearings, administer oaths, take testimony, and require (by subpena [sic] or otherwise) the appearance and testimony of witnesses and the production of records the Secretary considers advisable."); 15 U.S.C. § 2076(b)(3) (2009) ("The Commission shall also have the power . . . to require by subpena [sic] the attendance and testimony of witnesses and the production of all documentary evidence relating to the execution of its duties.").

266. *See* 49 U.S.C. § 30166(e) (2009) (The Secretary . . . reasonably may require a manufacturer of a motor vehicle or motor vehicle equipment to keep records, and a manufacturer, distributor, or dealer to make reports, to enable the Secretary to decide whether [it] has complied or is complying with this chapter or a regulation prescribed or order issued under this chapter.); 15 U.S.C. § 2065(b) (2009) ("Every person who is a manufacturer, private labeler, or distributor of a consumer product shall establish and maintain such records, make such reports, and provide such information as the Commission may, by rule, reasonably require for the purposes of implementing this Act, or to determine compliance with rules or orders prescribed under this Act.").

267. Consumer Product Safety Act, Pub. L. No. 92–573, 15 U.S.C. §§ 2051–2089 (2009).

268. *See* United States Department of Justice, Voting Section Litigation, Cases Raising Claims Under the Help America Vote Act (HAVA), http://www.justice.gov/crt/voting/litigation/caselist.php#hava (last visited May 2010).

269. VSTCPM, *supra* note 14 at 7.

270. *See* GAO Voting Systems Report, *supra* note 13 at 4-5.

271. VSTCPM, *supra* note 14 at 2.6.

272. *Id.* at 7.1.

273. *See e.g.*, GAO Voting Systems Report, *supra* note 13 at 31, *Hearing on the Election Assistance Commission: Hearing Before the Subcomm. on Elections of the House Committee on House Administration*, 110th Cong. (2008) (statement of Caroline Hunter, Vice Chair, Election Assistance Commission), *available at* http://cha.house.gov/UserFiles/82_testimony.pdf (stating that the EAC's power to decertify machines is limited to machines it has certified).

274. Bowsher v. Synar, 478 U.S. 714 (1986).

275. National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. No. 89–564, 80 Stat. 731 (1966) (codified as amended at 49 U.S.C. §§ 30101–70 (2009)).

276. 49 U.S.C. § 30165(a)(1) (2009).

277. *See* 15 U.S.C. 2069 (2009).

278. Presidential Statement on Signing the Help America Vote Act of 2002, Pub. Papers 1926 (Oct. 29, 2002), *available at* http://www.america.gov/st/washfile-english/2002/October/20021029140043gorin@pd.state.gov0.1174127.html.

279. *Id.*

280. *See* Contract No. 071B4200234 between the State of Michigan and Election Systems and Software, Inc. at 70 (May 24, 2004), *available at* http://accurate-voting.org/contracts/MI/MI_ess_2004.pdf; Contract Award No. NEG-21231, Group 22300 – Voting Systems and Related Services and Ballot Marking or Other Voting Devices Accessible to Individuals with Disabilities (Rev. May 9, 2008), *available at* http://www.panix.com/~burstein/NY_state_2008.pdf.

281. Much of this was adapted from the model contract in the New Jersey Public Advocate Report, *supra* note 186.

282. *See generally* New Jersey Public Advocate Report, *supra* note 186.

283. City Council R. 18A18-0238, 2009, Council Period 18 (D.C. 2009), 2009 D.C. Law L18-0103.

284. S.B. 1404, 2009-10 Reg. Sess. (Cal. 2010).

285. S.B. 541, 2009-10 Reg. Sess. (Cal. 2009).

286. *See* National Association of Secretaries of State, How States are Using Federal Funds to Carry Out the Help America Vote Act (HAVA) (2010), *available at* http://www.nass.org/index.php?option=com_docman&task=doc_download&gid=945.

287. This would be particularly important for states that do not require federal certification and rely on their own testing programs.

288. 42 U.S.C. § 15481 (a) (2009) defines a voting system as "(1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used— (A) to define ballots; (B) to cast and count votes; (C) to report or display election results; and (D) to maintain and produce any audit trail information; and (2) the practices and associated documentation used— (A) to identify system components and versions of such components; (B) to test the system during its development and maintenance; (C) to maintain records of system errors and defects; (D) to determine specific system changes to be made to a system after the initial qualification of the system; and (E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots)."

289. *See* Brennan Center for Justice, VRM in the States: Electronic Poll-Books, http://www.brennancenter.org/content/pages/vrm_electronic_poll-books (last visited Apr. 26, 2010).

290. *See, e.g.,* Mike Saewitz, *Chesapeake's electronic pollbooks were voting-delay villains*, The Virginian-Pilot, Nov. 6, 2008, *available at* http://hamptonroads.com/2008/11/chesapeakes-electronic-poll-books-were-votingdelay-villains, Mary Lou Pickel, *Countdown 2008: Computer Woes Slow Georgians at Polls*, The Atlanta Journal-Constitution, Oct. 28, 2008, *available at* http://www.ajc.com/services/content/printedition/2008/10/28/advancevote.html. T.J. Aulds, *No 'Super' Glitches Reported for New Voting System*, The Galveston County Daily News, Nov. 4, 2009, *available at* http://www.galvnews.com/story.lasso?ewcd=2dfb9d86700788db, Posting of Mike McPhee to denverpost.com, Ritter Victorious, Voters Struggle, http://www.denverpost.com/outdoors/ci_4616285 (last updated Jul. 9, 2009, 17:37 EST).

291. Definition from Technical Guidelines Development Committee, Voluntary Voting System Guidelines Recommendations to the United States Election Assistance Commission, Appendix A 6 (2007).

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

Renewing Democracy After Citizens United
Susan Liss, Michael Waldman

Small Donor Matching Funds: The NYC Election Experience
Susan Liss, Angela Migally

New Politics of Judicial Elections, 2000-2009: Decade of Change
James Sample, Adam Skaggs, Jonathan Blitzer

The Filibuster: Its Use and Abuse
Mimi Marziani

Voter Registration in a Digital Age
Christopher Ponoroff, edited by Wendy Weiser

User Fees for Criminal Justice?
Rebekah Diller

Buying Justice: The Impact of Citizens United *on Judicial Elections*
Adam Skaggs

A Citizen's Guide to Redistricting, Revised and Updated: 2010
Justin Levitt

Domestic Surveillance: New Rules, New Risks
Emily Berman

Domestic Counter-Terrorism and Radicalization
Faiza Patel

Corporate Campaign Spending: Giving Shareholders a Voice
Ciara Torres-Spelliscy

Foreclosures: A Crisis in Legal Representation
Melanca Clark with Maggie Barron

Racial Disparities in Federal Prosecutions
Brennan Center for Justice &
the National Institute on Law and Equity

For more information, please visit www.brennancenter.org

BRENNAN
CENTER
FOR JUSTICE

At New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
www.brennancenter.org