School of Law
UNIVERSITY OF GEORGIA
Prepare. Connect. Lead.

Journal of Intellectual Property Law

Volume 24 | Issue 2 Article 7

April 2017

Fundamental, Unequivocal, Yet Unreliable: The Interplay of Voting, Electronic Voting Systems, and Trade Secrets in Today's Interconnected World

Burns Marlow
University of Georgia School of Law

FUNDAMENTAL, UNEQUIVOCAL, YET UNRELIABLE: THE INTERPLAY OF VOTING, ELECTRONIC VOTING SYSTEMS, AND TRADE SECRETS IN TODAY'S INTERCONNECTED WORLD

Burns Marlow[*]

TABLE OF CONTENTS

[*] J.D. Candidate, 2018, University of Georgia School of Law; University of North Georgia, 2011, Bachelor of Science in Criminal Justice. The author would like to thank Dean Lori Ringhand and Chris Ramsey for their outstanding feedback and guidance on this Note.

I. INTRODUCTION

It was not too long ago that "no taxation without representation"[1] unified the American colonies to declare their independence from Great Britain. A simple desire for a voice in government empowered the political movement which laid the foundation for the Democratic Republic inhabitants of the United States enjoy today.[2] The signers of the Declaration of Independence pledged their lives, fortunes, and honor to a movement premised on representation in government.[3] The importance of the right to cast a ballot has been increasingly recognized since the Declaration of Independence.[4] Specifically, the United States Constitution grants citizens the ability to vote without discrimination in four amendments but does not expressly confer a right to vote.[5] The Fifteenth Amendment prohibits the denial of the right to vote on the basis of race.[6] The Nineteenth Amendment grants the right to vote to women.[7] The Twenty-Fourth Amendment prevents the use of a poll tax in all elections.[8] Lastly, the Twenty-Sixth Amendment grants the right to vote to United States citizens who are at least eighteen years of age.[9] While qualifications are generally left to individual states, Article One, Section Two of the Constitution mandates that the qualifications to vote in federal elections be the same as the requirements to vote in the largest branch of a state's legislature.[10]

But while our Constitution protects the *ability* to vote, significant legal protections ensuring the *accuracy* of a vote are lacking. Technological innovations and an emphasis on efficiency in elections has only exacerbated the problem. Since the passage of the Help America Vote Act (HAVA) in 2002, every state incentivized the utilization of an electronic voting machine in its election process.[11] In reaction to the 2000 Florida voting system debacle, Congress passed HAVA, allocating over three billion dollars to states for

---

[1] NCC Staff, *On the Day: No taxation without representation* (Oct. 7, 2016), http://constitutioncenter.org/blog/250-eyars-ago-today-no-taxation-withough-representation/.

[2] *Id.*

[3] THE DECLARATION OF INDEPENDENCE (U.S. 1776).

[4] Garrett Epps, *Voting: Right or Privilege?*, THE ATLANTIC (Sept. 18, 2012), http://www.theatlantic.com/national/archive/2012/09/voting-right-or-privilege/262511/.

[5] *Id.*

[6] U.S. CONST. amend. XV.

[7] U.S. CONST. amend. XIX.

[8] U.S. CONST. amend. XIV.

[9] U.S. CONST. amend. XVI.

[10] U.S. CONST. art. 1, § 2, cl. 7.

[11] HAVA, Pub. L. No. 107-252, 116 Stat. 1666 (codified at 42 U.S.C. §§ 20901–20906 (2006)).

purchasing and implementing electronic voting machines to improve the electoral process.[12]

In addition to allocating funding for technological improvements, HAVA also created an independent government agency to assist in certification and testing of voting systems known as the Election Assistance Commission (EAC).[13] The EAC is further tasked with providing *voluntary* guidelines on compliance with HAVA, after consultation with various election officials and stakeholders across the country which implement variable (albeit legal) electoral policies.[14] However, HAVA left the manner in which electronic voting machines were implemented to individual states and thus left nearly complete discretion to states to comply with the voluntary guidelines.[15] Additionally, certification responsibilities are shared both by states and the federal government to safeguard the effective operation of these voting systems, but detailed results of the testing is not publicly available.[16] The certification of these machines only mandates testing "a baseline of features, controls, and performance that a system should exhibit as part of an overall security strategy," and many federally certified machines have later malfunctioned.[17]

Thus, the EAC guidelines possess little authority in achieving the goals of HAVA. Former head of the EAC appointed by President Bush, DeForest Soaries called " 'charade' " and "claim[ed] that he had been deceived by both the White House and Congress" during his tenure, stating that "this country is ripe for stealing elections and for fraud."[18]

Despite its drawbacks, HAVA did facilitate slight regulation. Soon after the bill's passage, the EAC in conjunction with the National Institute of Standards and Technology crafted standards for electronic voting machines; however, compliance with these standards, in addition to testing and certification of these machines, is conducted by private companies referred to as Independent Testing Authorities (ITAs).[19] Furthermore, the results of the tests conducted

---

[12] *Id.*

[13] United States Electronic Assistance Commission, *Help America Vote Act*, https://www.eac.gov/about_the_eac/help_america_vote_act.aspx (last visited July 1, 2017).

[14] *Id.*

[15] *Id.*

[16] ERIC A. FISCHER & KEVIN J. COLEMAN, CONG. RESEARCH SERV., RL33190, THE DIRECT RECORDING ELECTRONIC VOTING MACHINE (DRE) CONTROVERSY: FAQS AND MISPERCEPTIONS 4 (2005).

[17] *Id.* at 10.

[18] Victoria Collier, *How to Rig an Election: The G.O.P. Aims to Paint the Country Red*, HARPER'S MAG. (Nov. 2012), http://harpers.org/archive/2012/11/how-to-rig-an-election/?single=1.

[19] Brian J. Miller, *The Right to Participate, the Right to Know, and Electronic Voting in Montana*, 69 MONT. L. REV. 371, 378 (2008).

by the ITAs are themselves proprietary, thereby protecting both the ITAs and the electronic voting system manufacturers under trade secret laws.[20] The testing results, plans, reports, recommendations for security measures, and electronic voting system reliability are inaccessible by the public.[21] If a security risk is discovered by the ITA relating to the vulnerability or reliability of the electronic voting machine, the ITA may write a report, "but only a small group of appointed individuals and the private vendor, not the general public, have access to it.[22] While the private companies essentially only have the burden of notifying the government of any impropriety in the security measures, these companies do not always meet this obligation.[23]

A. INFORMATION ON ELECTRONIC VOTING SYSTEMS

Beginning in the 1960s, computers and other software were first utilized in elections to "tabulate votes recorded on punch-card ballots."[24] Generally, individuals record their vote by "punching out a perforated hole with a stylus or pen," and the computer ballot box tabulates the vote according to position of the perforated hole and total number of votes in that position.[25]

As technology developed, three additional basic types of voting equipment developed in the United States: Optical Scan Paper Ballot Systems (manufactured by Diebold), Direct Recording Electronic Systems (DRE) (manufactured by Sequoia and ES&S), and Ballot Marking Devices and Systems.[26]

In optical scan systems, voters record their vote for a candidate or issue by "filling in an oval, completing an arrow, or filling in a box."[27] Many states utilize a paper record feature which allows for *some* of the DREs to "be equipped with Voter Verified Paper Trail (VVPAT) printers that allow the voter to confirm their selections on an independent paper record before recording

---

[20] *Id.* at 372.

[21] *Id.* at 378.

[22] *Id.* at 378–79.

[23] *Id.* at 379–80 (describing an experience in Indiana where ES&S installed unapproved software into the machines, and rather than notifying election officials, attempted to deceive the election officials and cover up the misfeasance by "reinstalling older, certified software 'under the guise of routine maintenance' ").

[24] Stephanie Philips, *Commentary: The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?*, 57 ALA. L. REV. 1123, 1124 (2006).

[25] *Id.* at 1124–25.

[26] Voting Equipment in the United States, VERIFIED VOTING FOUNDATION, https://www.verifiedvoting.org/resources/voting-equipment/(last visited July 1, 2017).

[27] *Id.*

their votes into computer memory," thereby preserving a paper trial which can be observed in audits in accordance with that state's laws.[28]

In 2003, leading electronic voting machine manufacturers aligned with the Information Technology Association of America to form the Election Technology Council (ETC).[29] With a goal to "raise the profile" of electronic voting and to identify security risks and technological malfunctioning, the association contains three major companies: Diebold, Sequoia, and Election Systems and Software (ES&S).[30] These companies' products are utilized throughout the United States and receive much of the spotlight surrounding electronic voting system criticism.[31]

Diebold is an optical scan voting system that records votes and tabulates total vote count in one unit called "The AccuVote-OS."[32] Voters use a pen provided by the polling station and fill in an oval for their preferred candidate.[33] If they wish to cast a write-in vote, voters must record that desire by marking an oval, or they must write the name of a write-in candidate.[34] Upon filling out the ballot, the voter takes it to the Accuvote-OS and the machine will record the selections. If an individual recorded too many votes in an individual contest, which is referred to as an "over-vote," the machine will allow the voter to correct their marks.[35] The only person to handle the ballot throughout this process is the voter.[36]

Sequoia manufactures a touch screen direct-recording electronic voting machine known as the "Sequoia AVC Edge."[37] Voters insert a "smart-card" into the machine which is issued by the poll worker and activates the machine.[38] Utilizing a 15-inch LCD touchscreen to navigate the ballot and record their votes, voters cast their ballot on a smart-card, and the machine records votes on

---

[28] *Id.*

[29] Carrie Jean Del Valle, *Historical Timeline of Electronic Voting Machines and Technology*, MEDIUM, https://medium.com/@carriedelvalle23/historical-timeline-of-electronic-voting-machines-and-technology-8a17f198f86.

[30] *Id.*

[31] Joel Roberts, *Can Voting Machines Be Trusted?*, CBS NEWS (Nov. 11, 2003, 3:11 PM), http://www.cbsnews.com/news/can-voting-machines-be-trusted/.

[32] Premier/Diebold (Dominion) AccuVote DS, VERIFIED VOTING FOUNDATION, https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-os/ (last visited July 1, 2017).

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] Sequoia (Dominion) AVC Edge, VERIFIED VOTING FOUNDATION, https://www.verifiedvoting.org/resources/voting-equipment/sequoia/avc-edge/ (last visited July 1, 2017).

[38] *Id.*

internal flash memory cards.[39] Upon making their votes, the smart-card is returned to a poll worker.[40] When the polls close, a poll worker transfers the vote tabulation information from the machine's internal flash memory card, and the information is taken to a central voter tabulation facility.[41] These machines may be activated to provide for a Voter Verified Paper Trail (VVPT) whereby the voter may confirm his choices by observing a paper receipt.[42]

In 2007, the California Secretary of State, Debra Bowen, conducted a mandatory statutory review of the voting tabulation systems utilized by California's polling precincts. The study reached three critical conclusions: (1) the certification standards of Sequoia machines were inadequate; (2) the Sequoia security measures were severely inadequate and could lead to questioning of the integrity of the election; and (3) the Sequoia machines suffer from numerous programming errors which could exacerbate the security concerns of the machines.[43] These security concerns include susceptibility to outside hacking whereby a motivated individual can easily circumvent the security measures and gain access to the machine's network.[44]

ES&S manufactures a DRE electronic voting machine similar to the Sequoia AVC Edge.[45] Utilizing an easily accessible touch screen interface and recording votes on an internal flash memory card, the ES&S "iVotronic" voting machine works similarly to a modern ATM whereby the voter manually selects their choices after the machine has been activated remotely from a supervisor terminal, known as the Personal Electronic Ballot (PEB), by a poll worker.[46] Like the Sequoia AVC Edge, the iVotronic allows the option for VVPT pending whether the State has implemented such auditing procedures, but that choice is entirely deferential to the state legislature and will not be possible unless that feature has been requested and installed.[47] Unlike the Sequoia AVC Edge, which prints voter results after they have completed the entire process,

---

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] State of California Secretary of State, WITHDRAWAL OF APPROVAL OF SEQUOIA VOTING SYSTEMS, INC., WINEDS V 3.1.012/AVC EDGE/INSIGHT/OPTECH 400-C DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF SEQUOIA VOTING SYSTEMS, INC., WINEDS V 3.1.012/AVC EDGE/INSIGHT/OPTECH 400-C DRE & OPTICAL SCAN VOTING SYSTEM 2–5 (Oct. 25, 2007).

[44] *Id.* at 4.

[45] Electronic Systems and Software (ES&S) iVotronics, VERIFIED VOTING FOUNDATION, https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/.

[46] *Id.*

[47] *Id.*

the iVotronic records *each change* the voter records, printing simultaneously that choice on a paper receipt that the voter can observe.[48] However, the security concerns of the iVotronic are especially compelling. Researchers recently discovered that the iVotronic had substantial vulnerabilities with one of its front magnetically-switched bidirectional infrared (IrDA) ports on the front of the machine and the memory devices utilized to access the machine.[49] Using that port and a PDA with a downloaded "PEB emulator," an individual could acquire access with ease.[50] Consequently, a voter who simply brings a magnet and a PDA could conceivably gain access to the machine's internal mechanisms or the poll supervisor's PEB and thereby obtain sensitive voter information and the opportunity to manipulate vote tabulation results.[51]

Electronic voting systems have been received with variable criticisms, while proponents argue that the machinery is incredibly secure, reliable, and flexible to the needs of an individual voter.[52] This Note will argue, however, electronic voting systems, as regulated today, give too much power over public elections to their private manufacturers.[53] Additionally, electronic voting machines such as DREs are susceptible to outside hacking and do not allow for reliable verification of votes.[54] Before passing HAVA, members of Congress attempted to pass amendments to the Act to ensure there were paper trails in case of technological failure, but neither passed.[55]

This Note will explore specific electoral events in places like Georgia with scattered reports throughout polling precincts in rural counties that the machines were "flipping" the vote to a different candidate in 2016, regardless of

---

[48] *Id.*

[49] Kim Zetter, *Report: Magnet and PDA Sufficient To Change Votes on Voting Machine*, WIRED (Dec. 17, 2007, 8:36 PM), https://www.wired.com/2007/12/report-magnet-a/.

[50] *Id.*; *see* Fig. 7.1.

[51] Zetter, *supra* note 49; *see* Fig. 7.1.

[52] *Do Electronic Voting Machines Improve the Voting Process?*, http://votingmachines.procon.org/view.answers.php?questionID=001290 (last updated Jan. 27, 2017, 10:28 AM).

[53] *Id.*

[54] *Id.*

[55] Brenda Reddix-Smalls, *Individual Liberties and Intellectual Property Protection – Proprietary Software in Digital Electronic Voting Machines: The Clash Between a Private Right and a Public Good in an Oligopolistic Market*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 689, 702–03 (2009) (citing S. 1487, 110th Cong. (2007) ("Senate bill '[t]o amend the Help America Vote Act of 2002 to require an individual, durable, voter-verified paper record under title III of such Act.' ")); H.R. REP. NO. 110-154, at 2 (2007) ("House Report accompanying '[a] bill to amend the Help America Vote Act of 2002 to require a voter-verified permanent paper ballot under title III of such Act, and for other purposes.' ").

the voter's selection.[56] Officials eventually concluded that the malfunctioning of the Bryan County machine occurred because "the county did not properly conduct logic and testing on [the machine]" to confirm that it would accurately capture a voter's choice.[57]

But the solution to resolving these deficiencies with electronic voting machines are complex. Trade secret law prevents electronic voting system manufacturers from divulging information on the proprietary software within these machines as long as certain requirements are met. While this does not prevent independent discovery of the software by a member of the public, this Note will elaborate on the substantial power these companies possess in dictating the outcome of the electoral process. Specifically, according to the United States Patent and Trademark Office (USPTO), as a member of the World Trade Organization, the United States must provide trade secret protection for companies that qualify.[58]

This Note explores electoral fraud history, statutory law, case law, and current issues painting doubt on the accuracy of the modern electoral system. Part II will discuss the specific instances of ballot fraud, HAVA's role in shaping the electronic voting system landscape, specific instances of critical electronic voting machine malfunctioning in elections, the public's response to these events, and recent events during the 2016 Presidential cycle.

Part III will discuss previously introduced solutions which, whether theoretical or actually implemented, fail to resolve the larger problem. This Note will then use specific examples from other areas of law to advocate the adoption of burden-shifting which will provide increased access to the electronic voting machines while simultaneously preserving the protection of a manufacturer's proprietary voting software under the UTSA. Part III will introduce burden-shifting's application to cases involving electronic voting systems and discuss Dr. Stein's efforts in Michigan and Pennsylvania during the 2016 presidential cycle. Part III will then make the argument for shifting the burden of proof. In Part IV, this Note will conclude that by shifting the burden of proof to the defendant after the plaintiff has made a sufficient evidentiary showing, courts can guarantee the accuracy of an election, and individuals will have the novel opportunity to hold electronic voting machine companies accountable for the malfunctioning of their machines.

---

[56] Kristina Torres, *Georgia Voting Machine Suspected of 'Flipping' Presidential Votes*, ATL-J. CONST. (Oct. 27, 2016), http://www.ajc.com/news/state--regional-govt--politics/georgia-voting-machine-suspected-flipping-presidential-votes/woKEUgpDDEyaw9o4J318XJ/.

[57] *Id.*

[58] *Trade Secret Policy*, UNITED STATES PATENT AND TRADEMARK OFFICE, https://www.uspto.gov/patents-getting-started/international-protection/trade-secret-policy (last visited July 1, 2017).

B. TRADE SECRETS APPLICATION

While these machines undoubtedly provide efficient returns on voting information and ease in calculating the percentage of votes cast for candidates and referendums, the technology still remains imperfect and prone to malfunctioning. Furthermore, the machines are manufactured by a small yet powerful number of manufacturers.[59] The solution seems simple: open the machine, test its software, and ensure that it did not malfunction. However, because of the Uniform Trade Secrets Act (UTSA) adopted by forty-eight states, this solution is not feasible.[60] Section 1.4 of the UTSA ensures that manufacturers do not willingly have to provide information about their software in these machines, thereby preventing an audit of their results.[61] Specifically, because the software is "not being generally known to and not being readily ascertainable by proper means," it represents economic value to the manufacturers and thereby is protected under the UTSA.[62] The most compelling reason manufacturers have for prohibiting inspection of these machines is that by placing their software into the public, the manufacturers lose the protections under the UTSA.[63] In sum, proprietary information protected under trade secret law is premised on three characteristics: "(1) not generally known to the public; (2) confers economic benefit to the company specifically because it is not generally known how" to manufacture the product; and (3) reasonable efforts may be used to maintain secrecy.[64]

Trade secret law's rationale is based on the notion that inventors and scientists will be more likely to pour significant resources and time into the development of their products if it is guaranteed that they will retain the economic value derived from its creation.[65] The law's vague, ambiguous nature allows the protections to apply to variable products within the intellectual property realm—essentially any discrete knowledge or information may be claimed to be a trade secret.[66] While the trade secret protection does not

---

[59] Roberts, *supra* note 31.

[60] Unif. Trade Secrets Act (Nat'l Conference of Comm'rs on Unif. State Laws, as amended 1985).

[61] *Id.* § 1.4.

[62] *Id.* § 1.4(i).

[63] *Id.* (see Comment to § 1).

[64] Paul Holly, *Trade Secrets and Election Companies: Private Companies in Government Elections*, IPWATCHDOG (Nov. 3, 2013), http://www.ipwatchdog.com/2013/11/03/trade-secrets-and-election-companies-the-use-of-equipment-manufactured-by-private-companies-in-government-elections/id=46002/.

[65] *Id.*

[66] *Id.*

prevent inventors from independently discovering a means to reproduce something protected under trade secret law, individuals and entities relying on trade secret law to protect their proprietary information enjoy the protection indefinitely—there is no temporal limit to its duration.[67]

In 1996, Congress passed the Freedom of Information Act to allow public access to government information.[68] Ensuring public trust in government was seemingly vital to Congress, but ensuring the integrity of elections was not a priority. Thus, the act contains exceptions for trade secrets to protect sensitive public and private information and interests.[69] Furthermore, disclosing information to the government, such as information surrounding the source code of the electronic voting machine, does not vitiate the trade secret protections; specifically, the fourth exception to the Freedom of Information Act allows "trade secrets and commercial or financial information obtained from a person and privileged or confidential" to be exempt from public disclosure requests.[70]

Proponents of amending the trade secret laws to allow access to the machines and disclosure of the software within should not expect to celebrate anytime soon. Congressman Hank Johnson of Georgia's fourth district recently displayed the bipartisan efforts to protect and bolster federal trade secret law by recently introducing the VOTE Act of 2016 "to amend the Help America Vote Act of 2002 to make improvements to voting system technology, election official training, and *protecting voting system source code*."[71] While the bill did not pass during the 114th Congress, the gesture is symbolic of the struggle electoral system reformers endure when attempting to hold the manufacturers accountable in the public domain.

Additionally, in May 2016, President Barack Obama signed the Defend Trade Secrets Act of 2016 into law, making the bill "the most significant trade secret reform in almost two decades."[72] Receiving overwhelming bipartisan support in both the House and the Senate, only two elected officials voted

---

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.* (citing the UTSA).

[71] VOTE Act of 2016, H.R. 5131, 114th Cong. (2016) (emphasis added). However, there have been bills introduced to require States to implement paper trails and other audit features which have received substantial support regardless of party; *see generally* The Voter Confidence and Increased Accessibility Act of 2005, H.R. 550, 109th Cong. (2005).

[72] Ehab Samuel, *What The Defend Trade Secrets Act Means for Businesses*, LAW 360 (May 11, 2016), http://www.law360.com/articles/791617/what-the-defend-trade-secrets-act-means-for-businesses.

against the bill.[73] Rather than preempting the variable trade secret laws amongst states which primarily follow the UTSA, The Defend Trade Secrets Act essentially creates a federal civil cause of action for the theft of trade secrets and adds additional layers of federal protection for individuals seeking to protect their works under trade secrets laws.[74] Therefore, the solution to potential electronic voting machine malfunctioning is unlikely to be resolved by Congress. Rather, their willful ignorance of a widely recognized electoral issue exacerbates the already prevalent problems with holding electronic voting system manufacturers accountable.

C. PRESENT RELEVANCE

Concerns with the integrity, accuracy, and security of the various electronic voting machines have been exacerbated by recent events in the 2016 presidential election cycle, namely the outside-hackings of the Democratic National Committee (DNC), Republican National Committee (RNC), and Russia's alleged attempts to intervene in the election cycle. These concerns are exacerbated when reports surfaced that "[n]early half of the states in the U.S. have recently had their voter registration systems targeted by foreign hackers, and four of those systems have successfully been breached."[75] In an interview with NPR, President Obama promised to take action against Russia for their attempts to influence the 2016 presidential election.[76] Meanwhile President Trump unequivocally has voiced his discontent with the accuracy of the intelligence reports, believing that the same individuals within the CIA are attempting to "delegitimize" his presidency.[77] However, despite his reasons for withholding approval of the intelligence reports, President Trump repeatedly called the 2016 general election "rigged," casting considerable concern over the legitimacy of what has been perceived as the most unique presidential election

---

[73] *Id.* (stating that the vote in the House voting for the Bill was 410–2, and the vote in the Senate was 87–0).

[74] *Id.*

[75] Mike Levine & Pierre Thomas, *Russian Hackers Targeted Nearly Half of States' Voter Registration Systems, Successfully Infiltrated 4*, ABC NEWS (Sept. 29, 2016), http://abcnews.go.com/US/russian-hackers-targeted-half-states-voter-registration-systems/story?id=42435822.

[76] Julie Hirschfeld Davis & David E. Sanger, *Obama Says U.S. Will Retaliate for Russia's Election Meddling*, N.Y. TIMES (Dec. 15, 2016), https://www.nytimes.com/2016/12/15/us/politics/russia-hack-election-trump-obama.html.

[77] *Id.*

in recent memory.[78] Those claims of "rigging" by Trump's campaign prompted the Carter Center, a renowned not-for-profit, nongovernmental agency that has observed over 100 foreign elections and assisted in implementing democratic principles, to release a statement and condemn those claims as "unfounded and irresponsible."[79] Further analysis of recent events after the 2016 presidential election, including actions by the Department of Justice (DOJ) and Department of Homeland Security (DHS) will be discussed at a later point.

The problems inherent with voting machines have not gone unnoticed by the popular electorate in Georgia. In October 2016, two polls conducted by the *Atlanta Journal Constitution* portrayed not only the historical importance of the 2016 election but also the negative attitudes voters have toward electronic voting systems.[80] In a sample size of 1,157 Georgians who were asked a multitude of questions via telephone, 82% of respondents noted that this election "matters a great deal" to the country's future, and a plurality of voters likewise expressed concern with whether their vote will be accurately counted this year.[81] Specifically, only 45% of respondents were very confident, with 33% somewhat confident, 13% not too confident, and 7% not confident at all.[82] These statistics show that a majority of voters (52%) lack a baseline level of confidence in the current accuracy of the 2016 presidential election.[83]

II. BACKGROUND

Voting: integral, sacred, and a requisite premise of a democratic republic. Ensuring that one's voice is actually being registered is a foundational element of a true democratic republic. Without a complete guarantee that votes are accurately counted, representative government becomes a façade, and accountability becomes an unattainable aim. Yet voting fraud is not a novel dilemma. In 1932, Huey Long successfully ensured the passage of amendments to the Louisiana Constitution that would further his financial interests.[84] While

---

[78] Jonathan Martin & Alexander Burns, *Officials Fight Donald Trump's Claims of a Rigged Vote*, N.Y. TIMES (Oct. 16, 2016), http://www.nytimes.com/2016/10/17/us/politics/donald-trump-election-rigging.html.

[79] Press Release, Carter Center, Carter Center Statement on the Integrity of U.S. Elections (Oct. 19, 2016), https://www.cartercenter.org/news/pr/us-elections-101916.html.

[80] Abt SRBI, *Poll of Georgia Voters, October 2016*, ATL.-J. CONST., http://www.myajc.com/october-2016-poll/ (last visited July 1, 2017).

[81] *Id.*

[82] *Id.*

[83] *Id.*

[84] Victoria Collier, *How to Rig an Election*, HARPERS MAG. (Nov. 2012), http://harpers.org/archive/2012/11/how-to-rig-an-election/1/.

acting as Governor of Louisiana, Long was unafraid to threaten and intimidate state legislators with diminished funding to their parishes if his policy objectives were not passed.[85] Long was eventually caught, and 513 election officials were indicted.[86] However, he utilized the Louisiana legislature to modify "the state's election law, giving ex post facto protection to the [election officials]."[87]

Fast-forward sixteen years. Then-Congressman Lyndon Johnson faced a difficult primary opponent to the United States Senate.[88] Three significant events occurred in this race. In the initial primary, neither candidate was able to reach the requisite majority of votes to be elected; however, in the subsequent primary-runoff, Johnson was reportedly trailing by 20,000 votes with only a few districts left uncounted.[89] One district, San Antonio, had overwhelmingly voted for his opponent in the initial primary by a ratio of 2:1; yet, Johnson carried San Antonio by over 10,000 votes that night.[90] Furthermore, rural counties in the Rio Grande Valley heavily voted for Johnson, diminishing his opponent's lead to a seemingly close margin victory of 854 votes.[91] However, the next day, election officials "discovered" a new and uncounted precinct.[92] To complicate matters further, the Rio Grande Valley districts not only returned more ballots, *they then corrected* those returns, adequately ensuring Johnson received enough votes to be elected.[93]

A. THE 2000 PRESIDENTIAL ELECTION

One of the most significant events questioning election integrity occurred during the 2000 presidential election in Florida.[94] The lack of sound, uniform election procedures across Florida contributed significantly to the election day debacle.[95] Individuals were regularly denied access to the polls throughout the state, ranging from misidentification issues labeling potential voters as "felons"

---

85 *Id.*

86 *Id.*

87 *Id.*

88 Martin Tolchin, *How Johnson Won Election He'd Lost*, N.Y. TIMES (Feb. 11, 1990), http://www.nytimes.com/1990/02/11/us/how-johnson-won-election-he-d-lost.html.

89 *Id.*

90 *Id.*

91 *Id.*

92 *Id.*

93 *Id.*

94 Philips, *supra* note 24, at 1125.

95 *Rights Commission's Report on Florida Election*, WASH. POST (June 5, 2001), http://www.washingtonpost.com/wp-srv/onpolitics/transcripts/ccrdraft060401.htm.

to the lack of compliance of many absentee ballots with Florida law.[96] Consequently, the Commission on Civil Rights found that Florida experienced a large "undervote"—the ballots were cast but the technology in the voting machine failed to register the votes.[97] The ballots that failed to register contained "hanging chads," meaning many of the ballots did not have completely punched holes for specific candidates.[98]

The Commission also discovered that the governor and secretary of state ignored mounting evidence and repeated pleas by state election officials for a potential malfunction of their electronic voting systems.[99] Further evidence, as reported by the Commission, demonstrated that African Americans were the most severely affected group. While accounting for 11% of the total voting-age population in Florida, the Commission found that 54% of African American voters were denied the ability to vote.[100] Specifically, the Commission determined the most dramatic undercount in the election was the nonexistent ballots of the countless unknown eligible voters, who were wrongfully purged from the voter registration polls.[101]

The presidential election of 2000 exhibits the potential implications for refusing to address a real problem that may not only be affecting the accuracy of a vote, but also potentially diminishes the influence of minority groups in the election process.

B. THE 2002 AND 2006 ELECTIONS

> "DRE systems experienced a number of problems already in the 2002 elections, and we see this only as the tip of the iceberg."[102]

Despite existing since the 1970s, Direct Record Electronic Voting systems have been increasingly utilized to combat the problems that arose with ballot-voting in the 2000 presidential election. In 2002, in response to the debacle that

---

[96] David Barstow & Don Van Natta Jr., *Examining the Vote: How Bush Took Florida: Mining the Overseas Absentee Vote*, N.Y. TIMES (July 15, 2001), http://www.nytimes.com/2001/07/15/us/examining-the-vote-how-bush-took-florida-mining-the-overseas-absentee-vote.html?_r=0.

[97] *See supra* note 95.

[98] Ari Berman, *How the 2000 Election in Florida Led to a New Wave of Voter Disenfranchisement*, THE NATION (July 28, 2015), https://www.thenation.com/article/how-the-2000-election-in-florida-led-to-a-new-wave-of-voter-disenfranchisement/.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] Verified Voting Foundation, http://votingmachines.procon.org/view.source.php?sourceID=000961 (last visited July 1, 2017).

occurred in the 2000 presidential election, Congress passed the aforementioned HAVA, funneling over three billion dollars to incentivize states to upgrade their voting technology by utilizing electronic voting machines.[103] These systems were in effect in Florida's 13th Congressional District during the 2006 election cycle.[104] Ironically enough, Kathrine Harris, the former Secretary of State for Florida during the 2000 presidential election, decided to leave her seat, and a hard-fought and tight race ensued between Democrat Christine Jennings and Republican Vernon Buchanan.[105] On the night of the election, Buchanan won by a slim margin of less than 400 votes.[106] However, election officials soon discovered that 18,000 voters had seemingly not voted in that specific congressional race in the 13th District despite voting for candidates running for the United States Senate.[107] The large undervote occurred despite election officials receiving advanced reports during early voting that the electronic voting systems were regularly failing to register ballots properly in the congressional race.[108] Overall, the undervoting figure accounted for approximately 13% of individuals who voted on Election Day and 17% of individuals who took part in early voting.[109]

The 13th Congressional District utilized an ES&S (DRE) voting system.[110] Manufacturers of this system, perhaps in their effort to safeguard their own credibility and legitimacy, inserted software which forced a voter to verify all of their votes at the end in a type of "summary" page, including the display of "no selection made" in red letters if the voter failed to vote for a contest.[111] But this was not a VVPT—a voter could navigate away from the "warning screen" by simply, either knowingly or unintentionally, confirming their options.[112]

Florida election officials had been made aware of the issues with the machines from ES&S, identifying problems with delayed responses which varied across each terminal and could not be remedied without a software update—an update promised but which never occurred before the 2006

---

[103] Reddix-Smalls, *supra* note 55, at 702.

[104] Jessica Amunson & Sam Hirsch, *The Case of the Disappearing Votes: Lessons from the* Jennings v. Buchanan Congressional Election Contest, 17 WM. & MARY BILL RTS. J. 397, 400–07 (2008).

[105] *Id.*

[106] *Id.* at 398.

[107] *Id.* at 398–99.

[108] *Id.* at 399; *see* Todd Ruger, *Voting Glitch Prompts Warning*, SARASOTA HERALD-TRIB., Nov. 5, 2006, at B1.

[109] *Id.*

[110] *Id.* at 400.

[111] *Id.* at 107.

[112] *Id.* at 401.

November general election.[113] Jennings filed suit in Florida and moved for the Circuit Court to allow him to access the ES&S source code, which would allow experts to examine the software and determine if any malfunctioning occurred.[114] However, Florida's evidence code provided for "a trade-secret privilege."[115] Under this law, "a person has the privilege to refuse to disclose, and to prevent other persons from disclosing, a trade secret owned by that person if the allowance of the privilege will not conceal fraud or otherwise work injustice."[116] Claiming this protection was unprecedented, and in a trade secrets dispute, the plaintiff must have a "reasonable necessity for the requested materials."[117] ES&S had the burden to show "good cause for protecting or limiting discovery by demonstrating that . . . disclosure may be harmful."[118] Following an evidentiary hearing on the determination of Jennings' "reasonable necessity" for discovery, the Circuit Court Judge denied access to the ES&S software, reasoning that it would "result in destroying or at least gutting the protections afforded those who own the trade secrets."[119]

Despite the general consensus amongst experts, researchers, and academics in the political science field that if the votes had been accurately counted Jennings would have won by 3,000 votes, Jennings was unable to legally compel discovery of the ES&S Software.[120] As two commentators noted, Judge Gary essentially concluded that the public's right to know what happened in the election was subordinate to ES&S's trade secret privilege.[121] Despite Florida law requiring a manual recount because Buchanan won by less than 1%, there was no "paper trail" incorporated into the electoral practice in that district; thus, if Jennings was unable to prove malfunctioning because of the trade-secret privilege granted to ES&S, she was left without a remedy to prove machine error.[122] The practical effect left voters in Florida's 13th Congressional District contemplating whether the correct individual was representing their interests in the House of Representatives.

---

113 *Id.*

114 *Id.* at 405–06.

115 *Id.* at 407.

116 FLA. STAT. ANN. § 90.506 (2006).

117 Sheridan Healthcorp, Inc. v. Total Health Choice, Inc., 770 So. 2d 221, 222 (Fla. Dist. Ct. App. 2000).

118 Am. Express Travel Related Servs., Inc. v. Cruz, 761 So. 2d 1206, 1209 (Fla. Dist. Ct. App. 2000).

119 Amunson & Hirsch, *supra* note 104, at 410 (citing Order on Motions at 3, Jennings, No. 2006-CA-2973, 2006 WL 4404531).

120 *Id.* at 413.

121 *Id.* at 410.

122 *Id.*

In 2002, Georgia and Alabama also allegedly experienced reliability issues with their electronic voting machines. In Georgia, both three-time incumbent State Senator Max Cleland and Governor Roy Barnes were defeated in their bid for re-election.[123] Georgia utilized the Diebold voting machines.[124] The outcome was unexpected, and a whistle-blower conceded that the machines had recently received undisclosed software patches.[125] However, they were installed incredibly late in the process and did not abide by Georgia law that required these patches be certified by the state.[126]

Because of much criticism revolving around its voting machines used in elections such as 2000 Presidential Election and 2002 Georgia Gubernatorial and Senate Races, Diebold initially attempted to retain its reputation by creating a subsidiary "Premier" for election products.[127] However, it then distanced itself from being in the electoral field, and recently sold its subsidiary.[128] But the lesson from Georgia is clear and only advances proponents' remedies: scrutinize all the software and, at bare minimum, have a contingency plan in place.[129]

Similar to the experiences of both Governor Barnes and Senator Cleland, Governor Don Siegelman (D) believed he had won re-election in the 2002 Alabama gubernatorial race. However, Baldwin County, a primarily republican district, reported that a glitch had given 6,000 additional votes to Siegelman.[130] Additionally, evidence existed that the machine might have been hacked and tampered with to skew the results.[131]

According to a 2005 Congressional report, this computerized method of voting is now the most popular voting method in the United States.[132] While the report determined that the DREs did not pose a significant threat to electoral legitimacy at the time, the authors explicitly stated concerns about "the

---

123 Adam Cohen, *A Tale of Three (Electronic Voting) Elections*, N.Y. TIMES (July 31, 2008), http://www.nytimes.com/2008/07/31/opinion/31observer.html.

124 *Id.*; *see also Diebold Voting Machine President Personally Delivered a Secret, Illegal Software Update*, NATIONAL ELECTION DEFENSE COALITION, https://www.electiondefense.org/georgia-2002-1/ (last visited July 1, 2017).

125 *Id.*

126 *Id.*

127 *Diebold Exits Voting Machine Business*, CBS NEWS (Sept. 4, 2009, 12:54 PM), http://www.cbsnews.com/news/diebold-exits-voting-machine-business/.

128 *Id.*

129 Cohen, *supra* note 123.

130 *Id.*

131 *Id.*

132 Fischer & Coleman, *supra* note 16,

lack of information about DRE security, especially in relation to other systems and other components of election integrity."[133]

C. COMMUNITY ACTIVISM

In 2006, Mr. David Mills, an attorney and registered voter in Shelby County, Tennessee, challenged the constitutionality of electronic voting machines under both the Tennessee Constitution and United States Constitution.[134] Shelby County required its citizens to vote on electronic voting machines which did not produce a VVPT or any similar record of the vote that individual casted.[135] In addition, if a discrepancy occurred and a voter wished to verify the candidate they voted for, poll workers had no ability "to review a questionable vote and determine the intent of the voter."[136] Mr. Mills' primary concern with electronic voting machines revolved around verifiable data surrounding the election that would be able to be accessed in the case of a recount, but because Tennessee didn't mandate VVPT, his vote was diminished in comparison to other counties that provided paper ballots.[137] The Court failed to agree, holding that there was insufficient evidence that the electronic voting machines utilized in Shelby County were disenfranchising voters.[138] The Court allowed the continued use of the electronic voting machines because of the deference provided to legislatures in creating election systems.[139] In addition, because the voter has no right to a "perfect voting system" and adequate safeguards exist to guard against malfunction, the electronic voting systems in place are sufficient mediums for recording and tabulating votes.[140]

Furthermore, in 2006, Maryland Governor Robert Ehrlich, a long-time supporter of the Diebold electronic voting machines used in his state, called for a paper ballot requirement.[141] Other states such as Georgia and Florida are considering sweeping changes to the way their machines are utilized and regulated.[142]

---

[133] *Id.*
[134] Mills v. Shelby Cnty. Election Comm'n, 218 S.W.3d 33, 34 (Tenn. Ct. App. 2006).
[135] *Id.* at 35.
[136] *Id.*
[137] *Id.* at 40.
[138] *Id.*
[139] *Id.* at 41 (citing Mooney v. Phillips, 118 S.W.2d 224, 226 (1938)).
[140] *Id.* at 41–42.
[141] Election Reform Malfunction and Malfeasance: A Report on the Electronic Voting Debacle, COMMON CAUSE (2005), http://www.commoncause.org/research-reports/National_062206_Malfuntion_and_Malfeasance_Report.pdf.
[142] *Id.* at 16.

Unsurprisingly, Hollywood did not miss the opportunity to dramatize public concern with the vote integrity throughout the early 2000s. Two significant movies, Recount (2008) and Man of the Year (2006), depicted the harsh reality of the reliability of unregulated electronic voting systems. Produced by HBO, Recount is a dramatized account of *Bush v. Gore* and dives into the key criticisms of the election: hanging chads, differing electoral policies, and partisan biases. Kevin Spacey plays Ron Klain, a key democratic strategist and trusted advisor to Democratic Presidential Candidate Al Gore. The movie portrays a legal sparring match between James Baker, played by Tom Wilkinson, and Kevin Spacey's Ron Klain and highlights critical moments of the campaign, including the moment the Supreme Court ruled against Gore.[143]

In *Man of the Year* (2006), Robin Williams plays a comedian who is convinced to run for president and surprisingly wins—but only because the fictional electronic voting machine company, Delacroy, manipulated the results to ensure his victory.[144] To many there was little doubt that "Delacroy" symbolized the election disasters "Diebold" experienced in the elections around that time.[145]

D. THE 2012 PRESIDENTIAL ELECTION

In 2012, electronic voting machines reportedly caused issues in Pennsylvania, Virginia, South Carolina, and Georgia.[146] A video from a polling location in Pennsylvania showed voting machines "flipping" a vote from Obama to Romney.[147] Machine breakdowns in Virginia caused up to five hour delays at the voting precincts, and South Carolina reported similar malfunctioning with their own electronic voting systems.[148]

Despite an academic emphasis on the negligent maintenance and unreliable nature of these machines, the mere potential of outside hacking and manipulation remains possible. In August 2016, the DHS contemplated whether to add the United States election system to its list of entities (such as

---

[143] *See* Roger Ebert, *Recount*, ROGER EBERT: REVIEWS (May 25, 2008), http://www.rogerebert.com/reviews/recount-2008.

[144] David Weigel, *The Forgettable Liberal Politics of Robin Williams*, SLATE (Aug. 12, 2014, 10:56 AM), http://www.slate.com/blogs/weigel/2014/08/12/the_forgettable_liberal_politics_of_robin_williams.html.

[145] Marybeth Kuznik, *Movie Review: Man of the Year*, VOTEPA.US, http://www.votepa.us/news/past-milestones/2006/movie-review-man-year (last visited Dec. 8, 2017).

[146] Mark Clayton, *Voting-Machine Glitches: How Bad Was It on Election Day Around the Country?*, CHRISTIAN SCIENCE MONITOR (Nov. 7, 2012), http://www.csmonitor.com/USA/Elections/2012/1107/Voting-machine-glitches-How-bad-was-it-on-Election-Day-around-the-country.

[147] *Id.*

[148] *Id.*

the already-present power grid and financial institutions) needing protection from cybersecurity attacks.[149] Jeh Johnson, then-Secretary of Homeland Security, noted that his department was "actively thinking" about the additional cybersecurity protections.[150]

Despite the Secretary's rhetoric about preventing outside hacking in elections, the DHS was recently accused of attempting to bypass Georgia's protected electoral database firewall without authorization by Secretary of State of Georgia Brian Kemp.[151] Soon thereafter, the DHS decided to classify the electoral system as "critical infrastructure."[152] Despite DHS rightly acting to protect the integrity of elections, it was already too late to enact adequate safeguards and protections in the 2016 election cycle. However, President Obama reiterated that there existed no credible evidence of outside vote tampering.[153]

Yet the potential ease in tampering with these machines is incredibly concerning. In 2007, a group of researchers at Princeton University hacked into a Diebold electronic voting machine and successfully changed the voting results by inserting certain software into the voting machine.[154] One year later, the same researchers only took seven minutes to install a computer program in an electronic voting machine "that steals votes from one party's candidates, and gives them to another."[155] That machine that was hacked was manufactured by Sequoia Advantage.[156] Presently, according to Roger Johnson, head of the vulnerability assessment team at Argonne National Laboratory, the Sequoia Advantage machine is used "in at least six states by 9 million voters," and the Diebold machine are "used in at least 20 states by 21 million voters."[157]

---

[149] Nicole Ogrysko, *DHS Considers Adding Election System as Critical Cyber Infrastructure*, FED. NEWS RADIO (Aug. 3, 2016, 4:40 PM), http://federalnewsradio.com/cybersecurity/2016/08/dhs-considers-adding-election-system-critical-cyber-infrastructure/.

[150] *Id.*

[151] Byron Tau, *Georgia Says Someone in U.S. Government Tried to Hack State's Computers Housing Voter Data*, WALL ST. J. (Dec. 8, 2016, 6:17 PM), http://www.wsj.com/articles/georgia-reports-attempt-to-hack-states-election-database-via-ip-address-linked-to-homeland-security-1481229960.

[152] Eric Geller, *State Officials Blast 'Unprecedented' DHS Move to Secure Electoral System*, POLITICO (Jan. 9, 2017, 11:03 AM), http://www.politico.com/story/2017/01/state-electoral-system-hacking-homeland-security-233349.

[153] *Id.*

[154] Gerry Smith, *Electronic Voting Machines Still Widely Used Despite Security Concerns*, HUFFINGTON POST (Oct. 22, 2012, 3:51 PM), http://www.huffingtonpost.com/2012/10/22/electronic-voting-machines-2012_n_1992992.html.

[155] *Id.*

[156] *Id.*

[157] *Id.*

E. THE 2016 PRESIDENTIAL ELECTION AND ITS AFTERMATH

In November 2016 Donald Trump defeated Hillary Clinton in a tight contest to become the forty-sixth President of the United States. President Trump was initially declared the clear winner, but in a number of jurisdictions, various electronic voting systems errors consequently led to profoundly long lines.

In Pennsylvania, four counties reported problems with a total of twenty-five electronic voting machines.[158] Many Republicans, Democrats, and computer scientists concede that problems with the aging machines are common in Pennsylvania, but the state's top election official, Pedro Cortes, declared that, regardless of the problems that occurred with the machines, "it appears that no votes were cast inaccurately and no voters were disenfranchised."[159] However, in Pennsylvania's Butler, Lebanon, Luzerne, and Westmoreland counties, Republicans reported that their votes for Trump flipped to Hillary Clinton—a tough reality exacerbated by the notion that these counties do not utilize paper trails thus making it impossible to perform a post-election audit.[160] Specifically, in Westmoreland County, GOP chairman Michael Korns stated in an interview "that about a dozen voting machines were taken offline because they had been recording votes for Clinton that had been intended for Trump."[161]

Furthermore, North Carolina experienced such widespread problems with their electronic voting systems that they made the decision to keep polls open in eight precincts in Durham County for between twenty and sixty minutes "to check in voters manually."[162] Specifically, election officials in Durham County experienced issues consisting of "software malfunctions with the laptops used to verify voter registration."[163] Counties were forced to switch to paper rolls, and at one precinct, voting stopped for two hours when the election site ran out of forms.[164] Nearly 40% of Durham residents are African Americans—a county which voted overwhelmingly for President Obama in 2012.[165] A similar experience occurred in Charlotte, where one individual attempted to vote for

---

158 Darren Samuelsohn et al., *Trump Seizes on Isolated Glitches to Fuel 'Rigged' Election Claims*, POLITICO (Nov. 18, 2016, 3:30 PM), http://www.politico.com/story/2016/11/2016-election-glitches-trump-230953.

159 *Id.*

160 *Id.*

161 *Id.*

162 *Id.*

163 Mark Abadi, *Widespread Voting Problems Were Reported in a Critical Swing State*, BUS. INSIDER (Nov. 8, 2016, 3:47 PM), http://www.businessinsider.com/north-carolina-voting-problems-2016-11.

164 *Id.*

165 *Id.*

Republican Donald Trump on his machine up to fifteen times before it finally registered.[166]

In Washington County, Utah, election officials endured problems with getting the electronic voting machines operational after they failed to work properly when the polls opened.[167] Utah Director of Elections Mark Thomas noted that the machines experienced programming errors.[168] Overall, only ninety-nine out of the 380 machines allegedly had their memory cards programmed properly, and voters were given paper ballots instead.[169] In Detroit, Michigan, voters were delayed when the machine which counted ballots malfunctioned at the beginning of Election Day.[170] Voters were told to leave their ballots in a secure box or wait for a technician to arrive to address the problem.[171]

Not long after confirmation of 2016 election results, Green Party Candidate Jill Stein launched a recount effort in Pennsylvania, Michigan, and Wisconsin, citing critical flaws in the states' electronic voting systems for reliability and accurately verifying votes.[172] Dr. Stein was successful in obtaining a recount in Wisconsin, but President Trump remained the winner.[173] Meanwhile, Michigan began the recount until a lower court in Michigan halted the recount, and a federal judge declined Stein's request for a recount in Pennsylvania.[174]

III. ANALYSIS

Presently, trade secret law protects electronic voting machine manufacturers from the forces disclosure of their proprietary information to the public, regardless of the likelihood that a particular machine malfunctioned. Consequently, the machines cannot be audited to determine their accuracy and reliability, thus incentivizing companies to hide their errors and mistakes, or as

---

166 *Id.*

167 Richard Wolf & Kevin McCoy, *Voters in Key States Endured Long Lines, Equipment Failures*, USA TODAY (Nov. 9, 2016, 1:09 AM), http://www.usatoday.com/story/news/politics/elections/2016/11/08/voting-polls-election-day/93201770/.

168 Associated Press, *Malfunctioning Voting Machines Prompt Switch to Paper Ballots in Southern Utah*, GLOBAL NEWS (Nov. 8, 2016, 5:42 PM), http://globalnews.ca/news/3053885/utah-voting-machine-malfunctions-prompt-switch-to-paper-ballots/.

169 *See* Wolf & McCoy, *supra* note 167.

170 *Id.*

171 *Id.*

172 Daniel Marans, *What Jill Stein's Recount Effort Actually Accomplished*, HUFFINGTON POST (Dec. 12, 2016, 6:49 PM), http://www.huffingtonpost.com/entry/jill-stein-election-recount_us_58507032e4b092f08685ff68.

173 *Id.*

174 *Id.*

mentioned previously, to attempt to patch the software glitches without notice to the individual state.[175]

A. CALLS FOR REMEDIES

Many keen observers of the electoral process have identified substantive errors with these machines and have called for procedural reform in the manner electronic voting systems are regulated and utilized. Remedies such as paper auditing, changing the optics in the machines, and the creation of a federal election commission which produces mandatory, rather than the voluntary guidelines proffered by the HAVA-created EAC.[176]

Another possible solution has been called the "No Government Trade Secrets Solution" where it is declared that a government trade secret "in any context is little more than a legal fiction, [and] trade secrecy theory and application are clarified and transparency, accountability, and deliberative democracy are not curtailed by trade secrecy."[177] Essentially, this remedy calls for vitiating electronic voting system manufacturers' objections and mandatory disclosure of their proprietary software, simply because the law would eliminate government trade secrets.[178] Proponents argue this bright-line rule, or lack thereof, facilitates a more transparent and accountable process.[179] A voting system manufacturer wishing to maintain their competitive edge in the industry would seek protection under patent law instead, and the information filed in the patent would be openly disclosed to the public after eighteen months, thereby alleviating any concerns inherent with non-disclosure of integral election software.[180] Yet, with the aforementioned recent support by Republicans for increased trade secret protections, their ability to retain control of both the House and the Senate, and the recent presidential election of Republican President Donald Trump, government trade secrets are unlikely to be completely nullified—even through a patent remedy.

Commentators have likewise advocated for the use of liberal discovery.[181] For example, in Georgia, trial judges in contested-election cases have "the power to do everything 'necessary and proper' to expeditiously hear and resolve

---

175 Amunson & Hirsch, *supra* note 104.

176 Philips, *supra* note 24, at 1158–60.

177 David S. Levine, *The People's Trade Secrets?*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 107 (2011).

178 *Id.*

179 *Id.*

180 *Id.* at 108.

181 *See* Amunson & Hirsch, *supra* note 104, at 418.

the dispute, including 'to compel the production of evidence which may be required at such hearing.' "[182] Similarly, in statewide elections, Illinois provides plaintiffs with the ability to request the examination of "records and equipment under the control of an election authority."[183] However, the competing concern that, "[i]n some circumstances, there may be risks to the electoral system itself if voting-machine source code becomes widely available" will likely ensure that election-contest statutes are not construed liberally to include proprietary software under federal trade secret protections.[184] Without the federal government's implicit consent of vitiating some protections inherent with federal trade secrets, state judges are unlikely to allow liberal discovery.

B. THE PAPER AUDIT (VVPT) REMEDY

A potential solution to deficiencies in the electronic voting systems could require Congress to mandate uniform paper auditing (i.e., VVPT), thereby instructing the voting machine issue the voter with a paper receipt indicating how each vote was cast. However, in the absence of procedures for observing the open source software within the electronic voting systems, VVPTs are unlikely to provide little assurance to vote integrity, masking the potential future malfunctions in a façade of transparency.

Paper audits have increasingly gained traction in states that attempt to reform their electronic voting systems, implementing audit procedures where votes are hand-counted on paper records and comparing them to originally recorded vote counts.[185] Acting largely as a prophylactic, these procedures are generally implemented via state legislation and require variable mandatory audits of a small percentage of votes cast.[186] Only sixteen states do not have paper auditing policies in place.[187] Because of the unwillingness of Congress to address the insufficiencies with electronic voting systems, states have widely implemented variable auditing policies and safeguards to preserve public confidence in the electoral system, whether codified by statute, existing as a policy or directive, as is the case in California, or providing a foundation which

---

[182] *Id.* (citing O.C.G.A. § 21-2-525(b) (2008)).

[183] *Id.* (citing 10 ILL. COMP. STAT. ANN. 5/23-1.6a (West 2003)).

[184] *Id.*

[185] Post Election Audits, VERIFIED VOTING, https://www.verifiedvoting.org/resources/post-election-audits/ (last visited July 1, 2017).

[186] *Id.*

[187] Editorial: *Electronic Voting is the Real Threat to Elections*, USA TODAY (Sept. 19, 2012, 8:45 PM), http://usatoday30.usatoday.com/news/opinion/editorials/story/2012-09-19/electronic-voting-fraud-security/57809062/1.

differs by population in each county.[188] Yet, a prophylactic only masks the potential software issues within these machines, and if doubts remain to both the integrity of these electronic voting machine manufacturers and their machines, a VVPT installed by these manufacturers provides little assurance of accuracy and reliability in one's vote.

During the 2016 legislative session, the North Carolina General Assembly passed HB 836 which defines a ballot "as a paper document marked by a voter either by hand or electronically," meaning that the over 300 iVotronic machines currently in use in Brunswick and Pender Counties will be non-compliant because the machines do not produce a ballot.[189]

Another swing state, Virginia, does not implement any auditing procedures.[190] Florida, while implementing an auditing procedure in 2007, audits only one randomly selected election contest which is selected separately in each county.[191] Pennsylvania instituted an audit requirement for 2% of the votes cast or 2000 votes, whichever is the lesser.[192] In addition, California, whose statutes and policies often blaze a trail and provide a sound model, only requires a hand count of ballots of 1% of precincts in each jurisdiction.[193] Meanwhile, in Connecticut, the General Assembly codified mandatory use of paper ballots and manual audits.[194] During each election, 10% of voting districts in Connecticut are randomly selected, and state officials conduct a hand count of the ballots.[195]

Imagine a grocery store in the early morning. Joe is standing in line, waiting patiently for the teenager at the cash register to slowly finish with the elderly lady in front of him. Joe's responsibilities and obligations begin to race through his mind, and he realizes he is going to be late for work. He still needs to fill up on gas, grab breakfast for the family, and take the dog outside. But finally, it is his turn. He hurriedly loads the items on the conveyor belt, pays for his purchase, takes his receipt, and rushes out the store.

---

188 *Id.*

189 Adam Wagner, *2015 Legislation in North Carolina Bans Strictly Electronic Voting Machine*, WILMINGTON STAR-NEWS (Sept. 6, 2016), http://www.govtech.com/policy/2015-Legislation-in-North-Carolina-Bans-Strictly-Electronic-Voting-Machine.html.

190 *See id.*; Post Election Audits, *supra* note 186.

191 *Id.*

192 *Id.*

193 *Id.*

194 Suzanne Mello-Stark, *Some States – Including Swing States – Have Flawed Voting Systems*, VOX (Nov. 3, 2016, 7:30 AM), http://www.vox.com/the-big-idea/2016/11/1/13486386/election-rigged-paper-trail-audit.

195 *Id.*

Now imagine that grocery store is a voting precinct, and the cashier is a volunteer election official. Arguably, the precinct also retains a copy of the receipt and has the ability to verify votes. The problem with VVPTs is axiomatic—a collective electorate cannot rely on individual voters to actually look at their receipt, or even for a volunteer election official to ensure each voter confirms their receipt. While VVPTs certainly diminish fear, they fail to provide complete transparency. Unless guided by electoral requirements or state statutes, the need to actually compare paper audits with the voting system's record is compelling evidence of corrupted software. If the software within an electronic voting system is, for example, "flipping votes," how can voters place complete trust in the VVPT feature if the software has been demonstrated to be corrupted?[196]

While these policies do assist in reassuring the public in the integrity of the electoral system, they do little more than divert public attention from the real problem: the auditing of the software. Thus, broadening the scope of auditing paper ballots and proposals to implement them further do little more than facilitate an unverifiable electoral system that promotes convenience over reliability.

C. THE LITIGANT'S SOLUTION: BURDEN SHIFTING

Past attempts at remedying the problems inherent with electronic voting systems have been met without success. The aforementioned remedies focus on legislation, ranging from the creation of a new commission to the complete nullification of government trade secrets. Yet, scholars and political commentators have failed to recognize an additional avenue for expanding access to the software within the machines: the practice of burden shifting. In legal issues revolving around compliance with Environmental and Administrative laws, burden shifting is commonly practiced.

Typically, a party bringing litigation has the burden of production and persuasion to produce evidence supporting its claim. In *McDonnell Douglas Corp. v. Green*, the Supreme Court deviated from that norm and created the burden-shifting framework which governs in employment discrimination claims.[197] In reaching its conclusion, the Court noted that it was the "purpose of Congress to assure equality of employment opportunities and to eliminate those discriminatory practices and devices which have fostered racially stratified job

---

[196] Reddix-Smalls, *supra* note 55, at 704.

[197] Adam Kielich, *The McDonnell Douglas Burden Shifting Framework*, THE KIELICH LAW FIRM, http://www.kielichlawfirm.com/the-mcdonnell-douglas-burden-shifting-framework/ (last visited July 14, 2017) (citing McDonnell Douglas Corp. v. Green, 411 U.S. 792 (1973)).

environments to the disadvantage of minority citizens."[198] Similar to electronic voting system cases where the plaintiff is unable to survive a motion for summary judgment because of the lack of knowledge of particularized evidence as a result of trade secret protection, many employment discrimination claims likewise fail to make it to trial.[199] Rather than force the party bringing the claim to engage in extensive and time-consuming discovery to find evidence to support their claim, the burden-shifting framework "shifts the burden to the employer to produce a nondiscriminatory reason. . . . [before] it shifts the burden back to the employee-plaintiff to disprove the alleged nondiscriminatory reason for the employer's conduct."[200]

The *McDonnell Douglas* framework requires three prongs be met:

> (1) The plaintiff must plead and prove a prima facie case of discrimination by a preponderance of the evidence; (2) The burden of production shifts to the employer to articulate a legitimate, nondiscriminatory motive for its conduct; [and] (3) The burden of production shifts back to the employee to prove the employer's provided motive is pretext for discriminatory conduct.[201]

Usually, the plaintiff bringing the action belongs to a protected group, and the framework is typically utilized in cases where the plaintiff's assertions are based on circumstantial evidence.[202]

Burden shifting has likewise been a mechanism used to lower the evidentiary burden inherent in cases involving environmental law. Plaintiffs struggled to overcome significant evidentiary burdens in order to maintain a claim, such as proving, for example, that a pollutant injured not only the individual bringing the claim but also the wider public in general.[203] This problem was exacerbated by the lack of uniform federal standards for regulating pollution and thus a heavy burden on parties seeking to protect the environment.[204] States were likewise unwilling to impose additional environmental protections in fear that their state would suffer consequences from big businesses which opposed

---

198 McDonnell Douglas Corp. v. Green, 411 U.S. 792, 800 (1973).
199 *See* Kielich, *supra* note 198.
200 *Id.*
201 *Id.*
202 *Id.*
203 Martin H. Belsky, *Environmental Policy Law in the 1980's: Shifting Back the Burden of Proof*, 12 ECOLOGY L.Q. 1, 6 (1984).
204 *Id.* at 10.

reform.[205] Furthermore, in each different locality, variable environmental laws were in effect; therefore, activists had to begin anew when seeking environmental protections in different places.[206] With increased public focus on environmental concerns, Congress finally began to pass legislation addressing critical environmental concerns, reasoning that "private litigation would not solve pollution problems [and] that state efforts were inadequate."[207] This should sound familiar.

To diminish the public's involuntary contact with harmful toxins and pollutants, California passed the "Safe Drinking Water and Toxic Enforcement Act of 1986," shifting the burden to manufacturers and businesses to give "clear and reasonable warning" to anyone exposed to known cancerous or toxic chemicals.[208] California delegated the regulation of those warnings to its Office of Environmental Health and Hazard Assessment which established thresholds to determine the significance of risk standards.[209] Thus, the burden rests on these manufacturers to provide adequate data demonstrating their compliance with those standards.[210]

California has utilized burden-shifting in other toxic tort contexts.[211] The Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) did not expressly provide for a burden-shifting mechanism, but courts have interpreted the law in that manner.[212] Once the plaintiff establishes that a defendant is a person falling within the ambit of liability in the Act, the defendant bears the complete "burden of disproving that its actions resulted in a release of hazardous substances."[213]

Burden-shifting wouldn't completely vitiate an electronic voting system manufacturer's trade secret—it would solely entail releasing enough information, protected by the safety of an *in camera* inspection, to alleviate any concern of specific malfunctioning with these machines. Likewise, because all machines are built with the same optics and presumably receive the same software updates, manufacturers would be incentivized to keep detail data logs of software patches and ensure uniform compliance with those standards. Burden-shifting would provide the best opportunity for ensuring the accuracy

---

205 *Id.*

206 *Id.*

207 Alexandra B. Klass, *Pesticides, Children's Health Policy, and Common Law Tort Claims*, 7 MINN. J.L. SCI. & TECH. 89, 137 (2005) (citing Cal. Health-Safety Code 25249.6 (2004)).

208 *Id.* at 137 (citing CAL. HEALTH & SAFETY CODE § 25249.6 (2004)).

209 *Id.* at 138.

210 *Id.*

211 *Id.*

212 *Id.* at 139.

213 *Id.* at 140.

of an election while simultaneously minimizing the trade secret infringement upon a manufacture—an infringement which should be encouraged in light of these manufacturers profiting on our democratic process.

D. THE 2016 RECOUNT: VOTING SYSTEMS AND ELECTION INTEGRITY

As evidenced by Stein's 2016 recount efforts and previously discussed voting system issues beginning in the early 2000's, most electoral cases of fraud and other computer irregularities are filed under state election laws rather than under federal statute.[214] These suits are often filed by losing candidates and seek recounts or new elections.[215]

While many different events leading to litigation over electronic voting systems were introduced earlier in this Note, perhaps the best example of a standard which could be utilized lies in Ohio common law. In November 1990, a tightly contested race in the state's attorney general race was determined by "less than one-quarter of one percent."[216] The losing candidate filed suit, alleging that the optical scanning machines in one county were poorly maintained and "in such [a state of] disrepair."[217] Furthermore, these machines were alleged to have recorded more votes than were actually recorded in the poll books.[218]

Determining it was bound by stringent Ohio precedent, the court required the losing candidate to prove two facts: "(1) that one or more election irregularities occurred, and (2) that the irregularity or irregularities affected enough votes to change or make uncertain the result of the election" by clear and convincing evidence.[219] The court determined that the losing candidate's conclusory allegations that several optical scanning machines either failed to record a vote or the machine's outright rejection failed to prove by clear and convincing evidence "that an irregularity occurred."[220] However, the losing candidate was successful in proving a discrepancy of the poll books as an irregularity by clear and convincing evidence, but he nonetheless failed to prove the second prong.[221] Consequently, the court determined the irregularity did

---

214 *See* Philips, *supra* note 24, at 1154.
215 *Id.*
216 *Id.*
217 *Id.* (alteration in original).
218 *Id.*
219 *In re* Election of November 6, 1990 for Office of Attorney General, 569 N.E.2d 447, 448 (Ohio 1991).
220 *Id.* at 459.
221 *Id.* at 463.

not directly influence the outcome of the election, and the losing candidate was left without a remedy.[222]

More recent efforts have met similar ends. While Stein eventually failed in her attempts for a recount in Pennsylvania, United States District Court Judge Diamond delivered a detailed thirty-one-page opinion outlining his reason for denying Stein's motion.[223] Stein alleged that, while the electronic voting systems identified Donald Trump as the winner, he failed to receive a majority vote from Pennsylvania citizens.[224] Seeking to review, among other requests, the electronic voting systems in six different counties, Stein presented an expert witness and four affidavits from experts exhibiting the vulnerability of these electronic voting systems.[225] Denying the motion, Judge Diamond labeled Stein's claims as outrageous and unnecessary.[226]

Stein's suit in Michigan met a similar fate. In the initial suit, Dr. Stein sought a preliminary injunction for certification of Michigan's results in order to conduct a recount.[227] Granting the request, Judge Goldsmith recognized the likelihood of irreparable harm voters in Pennsylvania could experience if results were not completely accurate, noting that a fair and accurate vote is the "bedrock of our nation."[228] Judge Goldsmith later dissolved the injunction, rejecting Dr. Stein's allegations of vulnerable electronic voting machines in Pennsylvania.[229] Stein, according to Judge GoldSmith, had not presented "evidence of tampering or mistake" but rather asserted speculative allegations about the "mere potentiality" of an unfairly conducted vote.[230]

E. PROPOSING A BURDEN-SHIFTING STANDARD

The standard cited by the Ohio Supreme Court, while not primarily utilized as a burden-shifting statute, provides a practical and easily applicable standard for use in electronic voting system litigation. This Note will evaluate three elements critical to the burden shifting analysis.

1. Occurrence of Irregularities. As both Judge Goldsmith and Judge Diamond exhibited in their recent decisions to deny Dr. Stein's recount efforts, specific evidence of corrupted or malfunctioning software is required to maintain a

---

222 *Id.*
223 *Id.*
224 Stein v. Cortés, No. 16-6287 (E.D. Pa. Dec. 12, 2016) (Westlaw).
225 *Id.* at *8, *29.
226 *Id.* at *31.
227 Stein v. Thomas, No. 16-14233 (E.D. Mich. 2016).
228 *Id.* at 5.
229 *Stein*, No. 16014233, at 7.
230 *Id.*

claim.[231] While specific evidence of wrongdoing ensures that voting system manufacturers do not spend the entirety of their time in Court, the evidentiary burdens experienced by litigants in conjunction with the trade secret laws which protect these manufacturers essentially ensure that these manufacturers remain unaccountable to public voters.

In light of the legal restrictions imposed by both state and federal trade secret law, courts should utilize a more pragmatic approach and recognize that plaintiffs will often cite specific errors with the software in the machine. Yet mere inability to initially observe the software to determine the true nature of the problem should not diminish the public importance of a definitive understanding of the legitimacy of an election. Specific circumstances can show a court by clear and convincing evidence that irregularities occurred in these voting systems.

As previously discussed, substantial occurrences of "undervoting" and "overvoting" at specific polling precincts provide a significant lapse in trust with the voting systems. While voting is anonymous, it surely may be presumed that, for example, 18,000 voters would cast a vote in the race for a congressional seat.[232] The results exhibit a potential devastating issue with the counting mechanisms, and it is difficult to conceive a rational argument for a different source of the problem.

Furthermore, verifiable instances of actual machine malfunctioning should give cause for courts to probe further for information on the operation of affected voting systems. Lawyers may litigate the facts and repeated occurrence of electronic voting system malfunctioning by, for example, showing that "flipping" votes unquestionably increases the likelihood of machine error. Unconceivably, in both the 2012 and 2016 presidential election, despite substantial media scrutiny on the errors of these voting systems, the significance of these events have gone unnoticed (or likely ignored) by Congress, state legislatures, and courts.[233]

2. Effect on the Outcome of the Election. Perhaps a fear of opponents to trade secret reform or the utilization of burden-shifting fear that increased access to the courts and the potential flood of litigation should deter a remedy that, while better guaranteeing accurate electoral results, would make the voting process much more bureaucratic. But a key idea of a true democracy should not be solely concerned with efficiency. Elections are important enough to subvert the

---

[231] *See* Stein v. Cortes, No. 16-6287, at 24-6 (E.D. Pa. Dec. 12, 2016); Stein v. Thomas, No. 16-14233, at 6–7 (E.D. Mich. 2016).

[232] *See* Amunson & Hirsch, *supra* note 104, at 400.

[233] *See* Torres, *supra* note 56; *see also* Orgysko, *supra* note 149.

inconvenience and potential costs associated with increased access as a result of burden-shifting.

Thus, upon a plaintiff proving the irregularities by clear and convincing evidence, the burden should switch to the defendant manufacturer(s) to provide tangible evidence that these machines (i) did not malfunction or (ii) did malfunction but did not affect the outcome of the election. Despite appearing daunting and ground-shaking, manufacturers can easily comply with the obligation. Keep in mind that the major companies belong to an association which promulgates guidelines and conducts independent, yet confidential, testing.[234] By compiling data on certification for the current year for the alleged malfunctioning machine, defendant manufacturers can easily controvert allegations by presenting this data to a court without revealing any proprietary software which could potentially forfeit their economic benefits.[235] Consequently, the ability to absolve liability with data from the independent testing would *actually ensure* proper certification procedures are followed.[236]

3. Public Policy. When courts interpret trade secret privilege, such as Florida's trade secret privilege in *Buchanan*,[237] courts often emphasize the significance of the economic benefits from proprietary software and the potential harm a manufacturer could endure by complying with court orders. Voting is undoubtedly a fundamental right, and typically, when a fundamental right is threatened, Courts have applied strict scrutiny to determine whether the State has a narrowly tailored, compelling interest in the practice that is being challenged. Why has such exacting scrutiny not been applied in these cases to at least fashion a workable, adequate remedy which meets the needs of both parties?

The current unreliable and unchecked voting systems utilized in elections represent the potential for a substantial, pervasive threat to the fundamental right of voting. While these manufacturers are protected and enriched through free elections, voters remain unaware of the legitimacy and credibility of an electoral outcome. If voting truly is a fundamental right and the bedrock of our democracy, protection of the substance must be perceived just as vital as the ability.

Environmental law activists experienced nearly the same problems proponents of voting system reform experience: lack of uniform federal standards, variable treatment among states, and evidentiary concerns.[238] However, a variation of burden-shifting was utilized to ensure that consumers

---

234 Miller, *supra* note 19, at 378.
235 Klass, *supra* note 208, at 137.
236 *See* Amunson & Hirsch, *supra* note 104, at 405–06.
237 *See* FLA. STAT. ANN. § 90.506 (West 2017).
238 *See* Belsky, *supra* note 204, at 9–10.

were made aware of the cancerous and toxic materials within certain products.[239] But warnings, in the context of electronic voting systems, have been demonstrated to fail to reach the public, and frankly, in a system where the only accountability these manufacturers have are to each other, voters deserve more transparency.[240]

IV. CONCLUSION

Election errors are not novel issues. However, a prerequisite to a democratic republic requires free, uninhibited elections. The current electoral climate conditions our ability to vote on an ignorance of the actual accuracy of the instruments utilized to record that vote. Thus, while our ability to vote may be fundamental and unequivocal, the substance of our vote—our specific exercise of endorsement for a certain direction for this country—remains inaccurate and consequently unreliable.

The unreliability of the electronic voting systems has been exacerbated by the near-uniform adoption of the Uniform Trade Secrets Act, limiting claimants' ability to have their experts observe the machines because of the economic benefit derived from the substantially confined knowledge of its proprietary information.

Thus, plaintiffs have failed, ranging from the 1990 Ohio attorney general contest to the infamous Bush-Gore Florida debacle to Dr. Jill Stein's recount efforts, to maintain a successful claim in holding voting system manufacturers accountable. Requirements that plaintiffs plead specific evidence in support of their allegations relegates many complaints to Judge Diamond's and Judge Goldsmith's characterization as speculative, conclusory, and ridiculous allegations.

While previous attempts at remedying the problem, such as vitiating trade secrets, utilization of paper audits, federally created commissions, and independent reviews, have proven inadequate, a remedy to a problem exacerbated by legislatures requires judicial activism; specifically, the application of burden-shifting.

While seemingly an extraordinary standard, burden-shifting has been utilized in environmental law and administrative law. In environmental law specifically, activists experienced many of the same problems that proponents of increased regulation of electronic voting systems face today: variable standards and the lack of a ruling body. Concededly, the legislature in California initiated burden-shifting, but unlike much of the natural conflicts facilitating the laws in

---

[239] *See* Klass, *supra* note 208, at 138.

[240] *See* Cohen, *supra* note 123.

California, electronic voting systems are aging, developing critical flaws which continue to surface prominently in each subsequent election. Despite the increased media attention and academic scrutiny of these machines, legislatures have refused to address the problem, and if they have, the perceived, ideal remedies have been (1) to strengthen trade secret laws and (2) implement meaningless paper audits.

Redefining the regulation of electronic voting systems requires the intervention of the judiciary. Irregularities exist in these voting systems, but the utilization of burden-shifting will renew faith in the electoral system by identifying those errors while simultaneously continuing to protect the proprietary information of these systems. Transparency does not require full disclosure and inventory of each widget and mechanism within these systems, but rather it requires tangible data and statistics describing the operation of these machines. For as long as the substance of a vote remains conditional on the pure ability of private electronic system manufacturers to make a substantial profit on free elections, the ability to cast one is meaningless.