

Rage Against the Machine?:
Assessing Election Administrators' Perceptions of Electronic Voting Systems*

Craig Douglas Albert
William Hatcher
Gregg R. Murray+
Alexander Schwarzmenn

Augusta University

ABSTRACT: Recently, the legitimacy of US elections and election systems has been questioned by those concerned about foreign interference and other malicious tampering, as well as those concerned about domestic election administration interference. While there is a rich literature on the mechanics of election administration and some research has investigated public perception of electronic voting systems and election legitimacy, much less has been done assessing the perceptions of election administrators. The present research seeks to fill this gap by addressing the question, “How do Georgia election administrators perceive the use of e-pollbooks for voter check-in?” We expect that election administrators will perceive e-pollbooks as increasing democratic legitimacy and election security. To demonstrate, this paper reports the results of an NSF-funded survey of Georgia county elections administrators regarding the security of electronic voter check-in systems and the perceptions of the trustworthiness and legitimacy of these and related election systems. The online survey, conducted two months before the 2024 general election, was distributed to all 159 Georgia county elections administrators. The IRB-approved survey asked the administrators about their perceptions of the security, reliability, ease of use, and fairness of several poll book and voter check-in systems and various characteristics of elections in their counties.

+ Corresponding author gmurray@augusta.edu

Introduction

Electronic voting systems are an integral component of modern electoral procedures and an essential part of any democratic society. Such systems are composed of several entities working in concert, the most important of which are “Voter Registration Systems”, “Election Management Systems”, “Voting Terminals”, and “Electronic Poll Books”. The first have been computerized for some time using well-understood database technologies. In the United States, following the problematic 2000 election in Florida, with serious issues were caused by the obsolete and flawed mechanical voting devices (e.g., punch cards that, in many cases, sometimes did not record the voters’ choice correctly due to “hanging” and “pregnant chads”), the Help America Vote Act of 2002 (HAVA) mandated a nationwide modernization of the voting infrastructure. This led to the broad adoption of computerized solutions for the next two components, Voting Terminals and Electronic Poll Books. Consequently, all 50 States initiated efforts to select and deploy electronic voting solutions.

While addressing problems associated with flawed voting methods, electronic voting solutions introduced new problems inherent in computerized solutions, such as security, reliability, and integrity. The private sector rushed to market with hastily created and often inadequately engineered solutions. The result was an adoption of products that suffered from severe flaws: poor engineering, lack of resilience against the most elementary tampering or simple misconfiguration, the illusion of safety from misuse of cryptography, and, in general, an under-appreciation for the complexity of the electronic election systems that need to be built as sophisticated and secure distributed systems.

The broad concerns surrounding the integrity and security of electronic election systems used in the last three Presidential Elections underscore the need for a rigorous approach to

designing and implementing all such systems. Careless use of technology can lead to significant (and even sensational) problems with basic computing infrastructure, and indeed, a few striking examples arise in the context of voting technology. Vulnerabilities in the design and implementation of electronic voting systems, in their use of cryptography, their logging capabilities, and communication software could be exploited by an attacker to alter the result of an election (Browley, 2025), (Davtyan, 2009 and 2012), (Jancewicz, 2013), (Kiayias, 2007 and 2007b), (Shvartsman, 2010). In fact, all electronic election systems that were made available for independent evaluations have been found to contain vulnerabilities.

Electronic Poll Books are systems that provide a key function that ensures that all eligible voters can cast their vote and cast it at most once; this is referred to as the “one voter, one vote” imperative. These systems are relatively new within the broad landscape of electronic election systems and are being widely adopted to replace the old manual processes. It is interesting that while the premature deployment of immature technology resulted in numerous documented cases of serious problems with voting terminals and election management systems, another component of the electoral process—Election Day voter check-in—still often relies on the often arcane manual solutions using paper pollbooks, i.e., printed voter lists. The questionable manual process can cause poll opening delays, long lines, and errors, possibly disenfranchising numerous voters (Aponte et al., 2015). Today, the adoption of electronic solutions is increasing rapidly. The emerging computerized solutions, “electronic pollbooks”, or “e-pollbooks”, are available from several vendors. While the integrity and security of these systems are paramount to the entire electoral process, vendors are again rushing to produce solutions based on naive premises and software fraught with deficiencies. Without a well-thought-out approach, the desire to modernize and ease the administrative process can again lead to the premature adoption of severely deficient

solutions. It is noteworthy that while the electronic tabulators used on Election Day are normally stand-alone systems, an e-pollbook system is conceptually more complex because it is inherently a dynamic distributed system where multiple check-in devices must operate in concert in providing “one voter, one vote” guarantee, with security and integrity, and despite possible failures and the resulting need to dynamically reconfigure this distributed system on the fly.

To address the challenges associated with the use of technology in the elections, following the 2016 Presidential Election, the National Academies of Sciences, Engineering, and Medicine (NASEM) appointed an ad hoc committee, the Committee on the Future of Voting: Accessible, Reliable, Verifiable Technology. NASEM published an extensive committee report, “Securing the Vote: Protecting American Democracy” (NASEM, 2018). The report summarizes its findings regarding e-pollbooks as follows.

“Eligible voters may be denied the opportunity to vote a regular ballot if pollbooks are inaccurate. Internet access to e-pollbooks increases the risks associated with the use of e-pollbooks to manage elections. Cyberattacks can alter the voter registration databases used to generate and update pollbooks. If pollbooks are altered by external actors, eligible citizens might, on election days, be denied the right to vote or ineligible individuals might be permitted to vote. Cyberattacks could also compromise the record of who actually voted on Election Day—or disrupt an election in numerous other ways. If an e-pollbook is connected to a remote voter registration database and there is no offline backup, a denial-of-service cyberattack could force voting to be halted.”

Among its recommendations, the report states that “Congress should authorize and fund” the development of “security standards and verification and validation protocols for electronic pollbooks.”

In recent years, public awareness has increased of the vulnerabilities present in electronic voting systems. Many jurisdictions have initially purchased electronic voting systems without considering the risks and with the assumption that computer solutions eliminate flaws present in older technologies without introducing new potential flaws. As the awareness increased, many

researchers and jurisdictions sought to mitigate the risks, e.g., by replacing relatively new systems with better-designed and more dependable systems (Maurya and Dwivedi 2024) and by better testing of e-voting machines (Crimmins, Halderman, and Sturt 2025). and by introducing post-election audits of equipment and ballots cast (U.S. Election Assistance Commission 2021). At the same time, the election officials have no choice but to use the existing electronic election systems, regardless of the risks and whether they trust the electronic systems. This study focuses on the election officials' perceptions of electronic voting systems. The study was initially motivated by the need to understand the perceptions of the electronic pollbook systems, and it ultimately expanded to study the broader perceptions of voting systems.

Literature: Electronic Voting Systems

Although the risk to electronic voting machines is well documented, there is little research on the risk associated with e-pollbooks. Thus, this section presents the relevant extant literature on e-pollbooks and election security and then proceeds to a larger discussion on vulnerabilities at a general level concerning electronic voting. We believe both avenues of literature are pertinent to the present paper as voters' and administrators' perceptions of e-pollbooks are likely partially informed by the overall perception of electronic voting. Despite their growing adoption as a crucial component of the electoral process, electronic poll books remain an underexplored topic in academic literature. Schwarzmann (2021) identifies several key vulnerabilities in the current implementation of e-pollbooks, including: (a) synchronization issues, which create a window of opportunity for bad actors to vote multiple times; (b) challenges in replacing malfunctioning devices, potentially leading to data loss; and (c) the risk posed by insecure systems connected to e-pollbooks, which may allow adversaries to intercept data and execute impersonation attacks.

These security risks contribute to broader privacy concerns associated with electronic voting systems. Popoveniuc, Kelsey, and Leontie (2011) highlight a specific issue: e-pollbooks, despite offering advantages over traditional paper poll books, have inadvertently recorded the sequence of voter check-ins. This unintended logging of voter order compromises ballot secrecy, thus raising privacy concerns. A 2023 report examining the usability and accessibility of electronic poll books outlines both the benefits and drawbacks of these systems. Quesenbery, Baumeister, and Dawkins (2023) highlight several advantages, such as faster check-in times, improved efficiency in directing voters to the correct polling location, greater accuracy in voter registration records, and a more streamlined process for updating voter rolls post-election. However, these benefits are counterbalanced by specific challenges, including uncertainties tied to adopting new technology, the extent to which poll workers accept and adapt to e-pollbooks, the financial burden of implementation, and lingering security concerns surrounding these digital systems. Murray and Albert (2025) find that while e-pollbooks are intended to streamline the voter check-in process, public trust in these systems remains mixed. The authors note the multidimensional nature of public attitudes regarding election systems and that attitudes are diverse and complex (Murray and Albert 2025, 14). Specifically concerning e-pollbooks, the authors write, “Most important in policy terms, the results suggest that electronic poll books reduce... perceptions of an election’s legitimacy” (Murray and Albert 2025, 13). How does the literature on voting technology generally compare to the brief literature on e-pollbooks?

Electronic voting, or e-voting/e-democracy, has become an important area of investigation in election studies and political participation. Important reasoning behind the surge in e-voting is the belief that as a society increases its electronic technology and systems concerning elections, the easier it becomes to participate in the electoral process, thus increasing political participation

of the electorate. For instance, LeRoux, Fusi, and Brown (2020, 6) find that both online election information and specific e-registration services have a direct, positive relationship with political participation in studying the association between local governments' online features and voter turnout. They assert that local governments "can be assured that each investment in information availability and new e-services will pay off in the form of greater voter turnout" (p. 6).

However, with the increase in e-voting and e-democracy, more specifically, and the increase in political participation more generally, comes the chance of increased distrust in the electoral processes and issues of discrimination. Both risk shifting public perceptions of an electoral process to one of illegitimacy, which, if widely held, could ring the death knell for democracy. For instance, LeRoux, Fusi, and Brown argue that moving an election system online may disproportionally and negatively affect underrepresented groups that have lower levels of education and income. Petitpas, Jaquet, and Sciarini (2021) demonstrate in a case-study of e-voting in Switzerland that there is some increase in participation with e-voting methods but for specific groups only. They find that e-voting mainly increases participation among persistent abstainers and occasional voters (2021, 9) but not among frequent voters. Additionally, e-voting technology might not be user-friendly for all voters or may come with a needed increase in technology-useability, so voting costs may increase, leading to a decrease in voter participation (Downs, 1957).

For instance, in making a case for end-to-end verifiability, an important feature of a secure and reliable voting system, Ryan, Schneider, and Teague (2015) note individual voters need to understand how to verify their vote during e-voting on top of system-wide random verification measures. This requires that voters are more heavily invested in the process and that the process must be simple enough for voters to understand and to feel motivated to perform in large numbers. Further, the authors cautioned that voters must know the process thoroughly without relying on

machine instructions. These instructions can be targeted for manipulation and hacking, giving voters improper information on verification measures. In this end-to-end verification process, “voters can privately create an encryption of their vote. All encrypted voters are posted to a public website, where voters can confirm that their vote is correctly recorded. The batch of encrypted votes is anonymized and decrypted in a universally verifiable fashion and can then be tabulated” (Ryan, Schneider, and Teague 2015, 61). Even with the benefit of this highly secure and reliable method increasing electoral legitimacy, one must wonder how many individuals the increased costs would dissuade from voting. As Mount (2020) notes, the more complex e-voting becomes, the more disincentivized voters may become. Considering the potential impact of e-voting on voters broadly and certain groups specifically, one must wonder if the risks outweigh the benefits?

Furthermore, there are more direct security threats to e-voting and electoral legitimacy. For instance, electronic systems are unlikely to be entirely secure from interference and hacking. In a classic essay on e-voting, Moynihan (2004) argues that while using information technology may be beneficial from an e-government perspective, that is, making services and information more accessible, there are significant risks associated with e-voting, and “the failure of e-voting technology has profound consequences for the reliability of and public confidence in our electoral system” (p. 515). He argues that increasing reliance on e-voting technology increases the risk of failed elections, increasing voter distrust in the electoral system. While advocates write about the benefits of e-government and e-democracy, for example, enhancing civic participation in the public sphere by making public information more accessible and by enabling civic discourse through webservices, many are not paying attention to the increased risk to the electoral process that results from converting e-democracy into direct e-voting (Moynihan 2004, 515). Moynihan describes the security issues apparent in e-voting technology including the direct recording

electronic machines (DRE). For instance, he suggests that there have been issues with residual votes (i.e., votes lost because of marking more than one candidate), programming errors, and machine tampering, “which in some cases reversed election results” (2004, 519). To combat this, Moynihan suggests using an open-source approach, including mandating voter-verified paper trails (2004, 525). Even with this policy solution, however, he notes that the reliability of e-voting may be increased but might not be enough to avoid error, and he concludes rather pessimistically that “there is no such thing as a completely secure electronic system” (Moynihan 2004, 526).

Bringing the literature fully into the digital age, Garnett and James (2020) note that cyber-elections are marked by: the new ontological existence of the digital, new flows of data and communication, rapid acceleration in the pace of communications, commodification of electoral data, and expansion of actors involved in elections (2020, 112). From this evolving information space within electoral politics, the dangers have increased significantly since 2004. In fact, Garnett and James argue that even with progress in enhancing democratic goals, the era of cyber-elections poses “major threats to the running of elections as the activities of actors and potential mismanagement of the electoral process could undermine democratic ideals” (Garnett and James 2020, 112). They note three main issues where e-voting threatens the democratic process: deliberative opportunities, equality of participation, and electoral management delivery.

Concerning threats to deliberative opportunities, Garnett and James note the deliberate dissemination of incorrect information to sway public opinion and behavior including dis/misinformation campaigns (2020, 117). One example they mention is: “If a malicious actor was able to access an EMB’s [(election management body)] website or social media account...they could easily provide false information or fake election results” (2020, 117). Adding to the threat is the personification of candidate accounts, which provides false information and produces deep-

fakes that appear to present a candidate falsely, unbeknownst to the constituent (2020, 117). Concerning equality of participation, they note specific threats to registration. Some of the most sophisticated tools meant to increase equal participation have been to increase the accessibility and accuracy of voter registration books, including biometric technology and online registration (2020, 118). However, they identify several problems with this technology, including poor infrastructure in certain areas that may produce inadequate electricity access during voting and poor network access (2020, 118), as well as security breaches, privacy concerns, and erasing or amending election results (2020, 119). Concerning electoral management delivery, in particular, internet voting, they note the specific threats that could be caused by malicious denial of service attacks as well as an oversaturation of the website by legitimate voters, both delaying if not preventing voter access (2020, 119). Finally, they mention that if one can vote electronically away from a physical location, there is no guarantee that a voter is not being directly influenced or intimidated into voting a certain way (2020, 119).

Issues also arise in deliberate voter suppression, where certain individuals can be micro-targeted with inaccurate information about the location of polling stations, eligibility requirements, and registration status concerns (2020, 119). In other words, although e-voting and e-democracy attempt to increase participation and access, there are significant threats to democratic governance, specifically within the realm of electoral legitimacy. These same issues apply to Garnett and James' third area of concern, electoral management delivery, including hacking voter registration rolls and election results and then selling information that has been compromised (2020, 121). This all makes it a possibility that a voter may not vote or even register to vote because of privacy concerns specifically associated with e-voter register system vulnerabilities (2020, 121). Privacy

concerns mount when there is any potential connection between a vote cast and the voter (Agate et al. 2021).

Johnson, Jones, and Clendenon (2017) note that as the types of voting methods have increased, there have been additional issues in voter confidence in e-voting scenarios. Issues affecting voter confidence in e-voting include issues with auditing e-voting machines, especially the lack of a paper trail and the fact that private companies own these machines and may not provide access to them. Additionally, Johnson and co-authors note that software running on these machines may be considered commercial. If so, they are not required by the Federal Elections Commission to be tested (2017, 341). Machine security is also a possible driver of low-confidence in election integrity for e-voting methods. They note that the Congressional Research Service found that some machines were subject to nefarious attacks from malicious code, including malware, viruses, and Trojan horses. They have found exploits on basic memory buffers and encryption errors (2017, 342) and “air gap” attacks that require a malicious actor to directly tamper with machines that could alter vote-choice (2017, 342). Multiple other security issues cause potential pitfalls in voter confidence in e-voting, and as the authors note, “A dilemma of security lies in the fact that every precinct and every state could be...conducting their elections using different processes and systems” (Johnson, Jones, and Clendenon 2017, 342). The scholars suggest that issues in influence may also correlate negatively with voter confidence in e-machines depending on the narrative in the media regarding connections between corporations and lobbyists or outside actors and the voting technology being used.

They note one case regarding a connection between George Soros and Smartmatic, a company that makes e-voting technology that “[highlighted] the potential for many voters to wonder if they could be confident that their vote was actually being cast for the candidate they

wanted when using a DRE” (Johnson, Jones, and Clendenon 2017, 343). Additional concerns affecting voter confidence are finances, in other words, states’ financial ability to replace, replenish, and update their e-machines, leading to significant consequences regarding inadequate maintenance. Finally, there are numerous concerns with the usability of e-voting technology and the overall complexity of human-computer interface considerations. Johnson et al. note, “Systems that are dynamically controllable, intuitively understood, and give the user options for input, legibility, and typography will be the most successful and accepted by the user” (p. 344).

Agate et al. (2021) note that several problems affect e-voting and electoral integrity. They share others’ concerns about confidence in voter verification and voter incoercibility (i.e., voters can vote freely without any external influence), without which “users might be forced to vote in a certain way, or deliberately decide to sell their vote to the highest bidder” (Agate et al. 2021, 3). E-voting also generates receipt-freeness, where “users cannot prove their vote after having cast it” (Agate et al. 2021, 3), which again relates to privacy and verifiability concerns. There is a relationship between these three variables that causes potential lessening of voter confidence and election integrity in e-voting. Essex and Goodman (2020, 167) provide an effective summary by suggesting that in Canada, where there are more lax regulations on cybersecurity and voting regulations for e-voting, there exists, “a tangible threat to electoral integrity, which could compromise electoral modernization, reduce public trust in elections, and stifle government legitimacy.” Now that a brief literature on e-pollbooks specifically and issues with e-voting more generally have been considered, this paper proceeds to an overview of the election administration.

Literature: Public Administration and Election Administration

The scholarly field of public administration has developed a rich collection of literature on how elections are administered in democratic nations. The literature has focused on how election

administration can be improved and some of the weaknesses of current systems (Brown et al., 2019). In the United States context, studies have examined the implementation of the Help America Vote Act of 2002 (Hale & Slaton, 2008), cybersecurity risks (Williamson et al., 2020), and the overall importance of effective election administration in a democracy, particular public trust in the system (Hale, 2023). Additionally, the literature has included studies examining the complexity and interdependency of election administration in the US and its over 89,000 local government units. (Hale & Slaton, 2008; Montjoy, 2008). Election administration is unique in the U.S. due to the complexity of multiple governmental units as part of the nation's federal system, whereas, in many other democracies, there are more centralized electoral processes (Montjoy, 2008), such a decentralized system demands effective public management.

The complexity of election administration in the US causes multiple opportunities for inefficiencies. Many of the governmental units administering elections are understaffed and lack expertise in the increasingly complex nature of data associated with elections (Brown, et al., 2019). The closeness of the 2000 US presidential election demonstrated issues associated with the degree of decentralization in the nation's election administration. The aftermath of the election led Congress to pass the Help America Vote Act of 2002 (HAVA), which attempted to provide support for state and local governments to build the capacity of their election systems. Early studies found that before HAVA, election administrators sought to build capacity through professional associations, their networks, and community partnerships (Hale & Slaton, 2008), and these are activities that administrators still attempt today. HAVA's support for resources and information and sharing and more recent reforms helped election administrators continue these capacity-building efforts (Hale & Slaton, 2008). However, research surveying election administrators have found that they have a bias in favor of using electronic voting mechanisms (Moynihan & Lavertu,

2011) but are cautious about the efficacy of federal government involvement in improving election administration in the US (Moynihan & Silva, 2008).

While studies have been concerned with the inefficiencies of election administration in the US, others have argued the decentralized structure protects democracy. Still, there is a concern for the ability of US governments, especially rural ones, to effectively manage elections with today's challenges of political polarization and growing cybersecurity threats (Brown et al., 2019). In such a governance environment, the answer to the problem is often building the capacity of government. Thus, it is not surprising that the focus on managerial capacity is a common theme in the election administration literature. Kropf and colleagues (2020) studied the residual vote rate in North Carolina, and found that managerial capacity, financial resources, and technology reduced issues associated with residual voting (Kropf et al., 2020, p. 733).

Even though election administration is robust in the US with little error given the complexity of the system, the public tends to have low levels of trust in US elections, compared to other democracies (Hale & Brown, 2020). And efforts to address this issue of low trust, through education and messaging on when and how to vote, have not significantly improved the public's trust in elections (Brown, et al., 2024). Additionally, the research on election administration has overlooked the need to survey frontline election managers and officials directly (Moynihan & Sliva, 2008). Thus, our paper expands the recent literature on election administration and public management in two ways by examining trust in election systems and surveying election administrators directly.

DATA

The survey was distributed to each of the 159 county election administrators in the State of Georgia by email approximately one week after sending them a hard copy letter of introduction to the survey by US mail. The survey was approved by the authors' institutional review board. The survey is presented in Appendix A. The first survey was completed September 18, 2024, and the last on March 19, 2025. In total, 55 administrators "completed" the survey (34.6%), of which nine (5.6%) refused to participate. This yields 46 surveys with full or mostly full responses. The mean completion time for those who answered questions was 8.0 minutes. Nineteen administrators completed the survey after the 2024 General Election. It is not surprising that the response rate was below 50% in our study because data security is a sensitive topic that may discourage respondents to participate (Norris et al., 2016) and often due to budget cuts, local governments have fewer resources to spend the time needed to complete surveys (Norris & Reddick, 2013). However, our study's response rate is robust compared to similar surveys of local public administrators (Hatcher et al., 2020).

The administrators reported there are between 1,800 and 655,000 registered voters in their counties with a mean of 61,608. Further, they reported voter turnout ranged from 10% to 83% with a mean of 64.6%. Fifty-two percent of administrators described their counties as "rural," 30% as "small town," 5% as "suburb," and less than 7% as "city." The vast majority (90.1%) of administrators indicated their constituents vote in-person during early voting with the remainder voting in-person on election day.

Analysis and Results

As this is an exploratory study, we base our analyses on basic univariate statistics. The first series of questions, following Moynihan and Lavertu (2012), asks the administrators to answer questions about the reliability, security, accuracy, and ease of use of ballot marking devices (BMDs), e-pollbooks, paper poll books, and tabulators. The scores ranged from “poor” (coded 1) to “excellent” (coded 7). Table 1 shows that Tabulators and E-pollbooks are rated highest overall, both with overall mean scores of 6.2. For reliability and security, Tabulators are the standout performers with scores of 6.4 and 6.5, respectively, markedly higher than the least performing Paper Pollbooks, which scored 5.0 in reliability and 4.8 in security. When assessing the accuracy of vote choice, Tabulators again lead with a score of 6.8, compared to Paper Pollbooks, which lag behind with a score of 4.8.

Table 1. Attitudes toward Certain Voting Technology

	<u>BMD</u>	<u>E-pollbook</u>	<u>Paper Pollbook</u>	<u>Tabulators</u>	<u>MEAN</u>
Reliability	6.5	6.1	5.0	6.4	6.0
Security	6.4	6.3	4.8	6.5	6.0
Accuracy Vote Choice	6.7	6.2	4.8	6.8	6.1
Accuracy Voter Info	5.5	6.4	4.9	5.9	5.7
Easy Poll Workers	5.9	6.2	4.5	5.9	5.6
Easy Voters	5.9	6.3	4.5	5.9	5.6
MEAN	6.1	6.2	4.8	6.2	

In terms of the accuracy of voter information, E-pollbooks are rated best, achieving a score of 6.4, while Paper Pollbooks remain the least effective with a score of 4.9. For ease of use, both by poll workers and voters, E-pollbooks score the highest at 6.2 and 6.3 respectively, contrasting with Paper Pollbooks which receive the lowest ratings with scores of 4.5 in both categories. In each dimension, paper pollbooks receive the lowest ratings.

The next series of questions asked about the availability and use of paper and e-pollbooks at voting locations. Approximately 90% of administrators reported a paper pollbook was available at each voting location. Thirty-four percent indicated their county used paper and e-pollbooks in parallel in the General Election, and 7% indicated they used a paper pollbook for some reason on Election Day. Finally, almost 60% of administrators reported they did not check-in a single vote using a paper pollbook, 11% indicated they checked-in at least some voters that way, and 7% indicated they checked-in all voters that way.

The next series, again following Moynihan and Lavertu (2012), asked about administrators' feelings about the effects of technology on government operations in general and more specifically about the effects on election administration. The scores ranged from "strongly disagree" (coded 1) to "strongly agree" (coded 7), with a middle category or "neither agree nor disagree." Table 2 reports the mean score for each measure. Overall, the mean scores for each are very similar, with a mean score for government operations of 5.5 and 5.6 for election administration.

Table 2. Attitudes toward the Benefits of Technology

Government Operations

Improve govt ops	5.6
------------------	-----

Outweighs risks govt ops	5.3
--------------------------	-----

Positive effect govt ops	5.6
--------------------------	-----

Election Administration

Improve elect admin	5.7
---------------------	-----

Outweighs risks elect admin	5.3
-----------------------------	-----

Positive effect elect admin	5.9
-----------------------------	-----

The last series of questions about election technology asks to what extent the administrators rely on several sources of information about voting systems: vendors, other election administrators, professional organizations, state election officials, and others. The scores ranged from “none” (coded 1) to “a great deal” (coded 6). Table 3 shows the administrators heavily rely on state election officials (mean 5.3), followed closely by other election administrators (mean 5.2) and least on the generic option “others” (mean 2.8).

Table 3. Sources of Information on Voting Systems

Vendors	4.4
Other election administrators	5.2
Professional organizations	3.7
State election officials	5.3
Others	2.8

Finally, the administrators answered several questions about themselves. The typical administrator who answered the survey was 54 years old. Approximately 70% were female and 27% male. A bit more than 40% have some college education, while 36% have a college degree, and about 10% have a high school or graduate degree. About 90% reported their race/ethnicity is white, and 10% reported black or African American. The typical administrator reported having about 9 years in their current election administrator position. Ninety-three percent indicated election administration is their primary job.

Conclusions

The analysis provides unexpected but interesting results. First, the difference in opinion held by the administrators or experts and the public is not strikingly from a macro-level, given that this is a clear finding in the public administration literature that public opinion often differs from the viewpoints of government experts (Raadschelders et al., 2011). However, an intriguing puzzle is presented when compared with the literature on voters' perceptions of e-pollbooks. Murray and Albert (2025), the scholars conclude that voter perception of e-pollbooks decreases the legitimacy of elections and demonstrates that voters have a negative perception of e-pollbooks. One can extrapolate from this finding that voters generally negatively perceive voting technology. If that is the case, the results of the current study present a dilemma: why do electoral administrators typically have an overall favorable perception of e-pollbooks and voting technology while voters have the opposite understanding? What is the disconnect? What does this mean for electoral politics generally, and what will the future of electronic voting machines and democracy be like as the US moves closer to this voting methodology? One reason may be the fact that county administrators admit that their knowledge of e-voting comes mostly from state-level officials. This

could be because some form of partisan politics influences the overall opinions and ideas about e-pollbooks and electronic voting. This is an area of future research: does political ideology affect attitudes about the legitimacy of electronic voting machines?

Another consideration may be that administrators are more concerned with efficiency in elections rather than trust or legitimacy in government since they represent the government. Voters tend to see a decline in trust in government concerning electronic voting, especially when considering the possibility of vulnerabilities and secure methods of electronic voting (Murray and Albert 2025). Thus, does the nature of the role played by administrators cause the difference in perception between voters and administrators? Again, this is a further avenue of research to approach. The present research finds that county administrators have a positive perception of voting technology, specifically, a positive perception of e-pollbooks, especially relative to paper pollbooks. Thus, it is likely that Georgia will see and follow the general pattern of most US states to move toward greater electronic methodology in the electoral process. But with the disconnect between local officials and voters, how will the rise of the machines influence government legitimacy and democratic governance in the decades to come?

Appendix A. The Survey

INTRODUCTION/CONSENT*

Dear Georgia County Election Supervisor:

You are invited to participate in a research survey regarding voting technology in Georgia. This study is sponsored by the Augusta University School of Computer and Cyber Sciences and funded by the National Science Foundation. The survey takes about 15 minutes to complete.

The results will be used to understand the use of voting technology in Georgia. We plan to share the results in scientific journals and at scientific conferences with the hope the results will be useful for elections administrators, voters, and researchers.

There are no known risks to you from taking this survey. There is no direct benefit to you for participating, although we will provide participants with a report summarizing the findings with the hope that the information will offer insights that may be beneficial in your work and future decision-making regarding voting technology.

Responses will be kept strictly anonymous. Before completion of the study, all data will be stored in a password-protected electronic format. After completion of the study, versions of the data, with all identifying information removed, will be made available in a public online database for inspection and re-analysis so that other researchers can evaluate it. While the results of this study will be used for scholarly purposes only, they may be shared with Augusta University representatives.

Your participation is voluntary and there is no penalty if you do not participate. You are not required to answer all the questions. If you have questions or concerns about the survey or would like to receive a summary of the findings, please contact me as indicated below.

If you have any questions or concerns about the “rights of research subjects,” please contact the Augusta University IRB Office at (706) 721-1483.

Sincerely,

Gregg R. Murray, Ph.D.
Professor of Political Science
Department of Social Sciences
Augusta University
gmurray@augusta.edu
(706) 737-1710

Clicking on the “agree” button below indicates that:

- you have read the above information

- you voluntarily agree to participate
- you are at least 18 years of age

If you do not wish to participate in the research study, please decline participation by clicking on the “disagree” button.

AGREE
DISAGREE

WARM-UP QUESTION:

The first question is to verify your eligibility to complete the survey.

Are you the County Election Supervisor in your county?

Yes

No [terminate]

How would you describe the county for which you administer elections?

- Rural area
- Small town
- Suburb
- City

Approximately how many registered voters are in your jurisdiction? _____

What is the approximate voter turnout in your jurisdiction in presidential years?

_____ % **How do most voters in your jurisdiction cast their vote?**

- In person at the polling place on election day
- In person during early voting
- By mail

How would you rate ballot marking devices* (BMDs) on the following characteristics?:

[randomly rotate]

(1 = poor... 7 = excellent)

A. Reliability

B.

- C. Security
- D. Accuracy of recording voters' choices
- E. Accuracy of recording voters' information
- F. Ease of use by poll workers
- G. Ease of use by voters

* Also ask about: [randomly rotate]

- 1. e-pollbooks
- 2. manual paper pollbook process
- 3. BMDs
- 4. Tabulators

At the last election, was a paper pollbook available at each polling location on election day?

- yes
- no

At the last election, did your jurisdiction use electronic and paper pollbooks in parallel?

- yes
- no

At the last election, did your jurisdiction use the manual paper pollbook process for any reason on election day?

- yes
- no
- in part

At the last election, approximately what percentage of voters did you check in using paper pollbooks?

0% - 10% - 20% - 30% - 40% - 50% - 60% - 70% - 80% - 90% - 100%

To what extent do you disagree or agree with the following statements?

[randomly rotate]

(-3 = strongly disagree, 3 = strongly agree):

- A. The use of new information technologies can significantly improve the way government operates.
- B. The use of new information technologies can significantly improve the way elections are administered.
- C. The benefits of new technologies to the way government operates significantly outweigh the risks.

- D. The benefits of new technologies to election administration significantly outweigh the risks.
- E. Overall, the broad use of new information technology has a positive effect on the way government operates.
- F. Overall, the broad use of new information technology has a positive effect on the way elections are administered.

Now, a few questions about you and your job.

In what year were you born? _____

What is your gender?

- Female
- Male
- Something else

What is the highest level of school you have completed or the highest degree you have received?

- Less than HS
- HS
- Some College
- College
- Graduate

Which of the following categories best describes you? You may choose more than one. -

- White
- Black or African-American
- Hispanic
- American Indian or Alaska Native
- Asian
- Native Hawaiian or other Pacific Islander

How long have you served in any position in election administration?
_____years

How long have you served in your current position in election administration?
_____years

Is election administration your primary job?

- yes
- no

On average, what percentage of your work time do you spend on election and election-related duties?

0% - 10% - 20% - 30% - 40% - 50% - 60% - 70% - 80% - 90% - 100%

To what extent do you rely on the following sources of information about voting systems?

[randomly rotate]

(0 = no reliance, 10 = a great deal of reliance):

- A. Vendors
- B. Other election administrators
- C. Professional organizations (eg National Association of State Election Directors, Natl Association of Secretaries of State)
- D. State election officials
- E. Others _____

What new technological feature or features, if any, would help you administer your elections more securely, reliably, accurately, and/or easily?

THANKS AT END

Thank you very much for completing this study. Your answers have been recorded. On behalf of Augusta University and the National Science Foundation, thank you for being a part of this important research.

References

- Agate, Vincenzo, Alessandra De Paola, Peirluca Ferraro, Giuseppe Lo Re, and Marco Morana. 2021. "SecureBallot: A Secure Open-Source e-Voting System." *Journal of Network and Computer Applications* 191(October): 103165.
- Bromley, T., P. Reeves, and A. Shvartsman. 2025. Elections, technology, and the pursuit of integrity: the Connecticut landscape. In *State Certification Testing of Voting Systems National Conference, Indianapolis*, Indianapolis, IN, June 2012.
- Brown, M., Hale, K., Jordan, S., & Williamson, R. D. (2024). Restoring Trust in US Elections through Effective Election Administrator Messaging. *Public Opinion Quarterly*, 88(SI), 632-655.
- Brown, M., Hale, K., & King, B. A. (2019). *The future of election administration: Cases and conversations* (p. 266). Springer Nature.
- Crimmins, Braden L., J. Alex Halderman, and Bradley Sturt. "Improving the Security of United States Elections with Robust Optimization." *Operations Research* 73, no. 1 (2025): 61-85.
- Davtyan, S. Kentros, A. Kiayias, L. Michel, N. Nicolaou, A. Russell, A. See, N. Shashidhar, and A. A. Shvartsman. (2009). Taking total control of voting systems: firmware manipulations on an optical scan voting terminal. In *Proceedings of the 2009 ACM Symposium on Applied Computing, SAC '09*, pages 2049–2053, New York, NY, USA, 2009. ACM.
- Davtyan, S., A. Kiayias, L. Michel, A. Russell, and A. A. Shvartsman. (2012). Integrity of electronic voting systems: Fallacious use of cryptography. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing, SAC '12*, pages 1486–1493, New York, NY, USA, Mar. 2012. Association for Computing Machinery.
- Downs, Anthony. 1957. *An Economic Theory of Democracy*. HarperCollins, New York.
- Essex, Aleksander, and Nicole Goodman. 2020. "Protecting Electoral Integrity in the Digital Age: Developing E-Voting Regulations in Canada." *Election Law Journal* 19(2): 162-179.
- Garnett, Holly Ann, and Toby S. James. 2020. "Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity." *Election Law Journal* 19(2): 111-126.
- Hale, K. (2023). The Mechanics of Democracy: The Critical Role of Local Governments in Supporting Election Operations. In *Local Government Administration in Small Town America* (pp. 61-77). Routledge.
- Hale, K., & Brown, M. (2020). *How we vote: Innovation in American elections*. Georgetown University Press.

- Hale, K., & Slaton, C. D. (2008). Building capacity in election administration: Local responses to complexity and interdependence. *Public Administration Review*, 68(5), 839-849.
- Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy*, 5(2), 302-325.
- A. Aponte, J. Cruz, C. Jennings, D. MacDonald, and S. Wooden. Committee of Inquiry Report of Factual Findings. Tech. Rep. City of Hartford Court of Common Council, 2015.
- Jancewicz, R. J., A. Kiayias, L. D. Michel, A. Russell, and A. A. Shvartsman. (2013). Malicious takeover of voting systems: Arbitrary code execution on optical scan voting terminals. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing, SAC '13*, pages 1816–1823. ACM, 2013.
- Johnson, Nathan, Brian M. Jones, and Kyle Clendenon. 2017. “e-Voting in America: Current Realities and Future Directions.” In, Gabriele Meiselwitz (Ed.), *Social Computer and Social Media: Human Behavior*, pp. 337-349.
- Kiayias, A., L. Michel, A. Russell, N. Sashidar, A. See, and A. A. Shvartsman. (2007). An authentication and ballot layout attack against an optical scan voting terminal. In R. Martinez and D. A. Wagner, editors, *2007 USENIX/ACCURATE Electronic Voting Technology Workshop, EVT'07, Boston, MA, USA, August 6, 2007*. USENIX Association, 2007.
- Kiayias, A., L. Michel, A. Russell, N. Shashidhar, A. See, A. Shvartsman, and S. Davtyan. (2007). Tampering with special purpose trusted computing devices: A case study in optical scan e-voting. In *Computer Security Applications Conference, 2007. ACSAC 2007. Twenty-Third Annual*, pages 30 –39, dec. 2007.
- Kropf, M., Pope, J. V., Shepherd, M. J., & Mohr, Z. (2020). Making every vote count: The important role of managerial capacity in achieving better election administration outcomes. *Public Administration Review*, 80(5), 733-742.
- LeRoux, Kelly, Federica Fusi, and Adrian G. Brown. 2020. “Assessing e-Government Capacity to Increase Voter participation: Evidence from the U.S.” *Government Information Quarterly* 37(3): 101483.
- Maurya, Alka, and Rajendra Kumar Dwivedi. "Designing a secure large scale e-voting system leveraging sharding blockchain with interoperability protocol and consensus mechanism." In *2024 international conference on intelligent and innovative technologies in computing, electrical and electronics (IITCEE)*, pp. 1-7. IEEE, 2024.
- Montjoy, R. S. (2008). The public administration of elections. *Public Administration Review*, 68(5), 788-799.

- Mount, Michelle. 2020. "Innovations in Internet Voting Systems." *Georgetown Law Technology Review* 4(2): 699-710.
- Moynihhan, Donald. 2004. "Building Secure Elections: E-Voting, Security, and Systems Theory." *Public Administration Review* 64(5): 515-528.
- Moynihhan, D. P., & Lavertu, S. (2012). Cognitive biases in governing: Technology preferences in election administration. *Public administration review*, 72(1), 68-77.
- Moynihhan, D. P., & Silva, C. L. (2008). The administrators of democracy: A research note on local election officials. *Public Administration Review*, 68(5), 816-827.
- Murray, Gregg R., and Craig Douglas Albert. "In cyber we trust? Understanding election legitimacy in the age of electronic election systems." *Journal of Information Technology & Politics* (2025): 1-17.
- Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2021). Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity. *Journal of Urban Affairs*, 43(8), 1173-1195.
- Norris, D. F., & Reddick, C. G. (2013). Local e-government in the United States: Transformation or incremental change?. *Public Administration Review*, 73(1), 165-175.
- Williamson, R. D., Hale, K., & Brown, M. (2020). Security and integrity: Administrative structure, capacity, and American elections. *Journal of Political Institutions and Political Economy*, 1(2), 189-207.
- NASEM. (2018). *Securing the Vote: Protecting American Democracy*, September 2018. National Academies of Sciences, Engineering, and Medicine. (<https://nap.nationalacademies.org/catalog/25120/securing-the-vote-protecting-american-democracy>)
- Petitpas, Adrien, Julien M. Jaquet, and Pascal Sciarini. 2021. "Does E-Voting Matter for Turnout, and to Whom?" *Electoral Studies* 71 (June): 102245.
- Popoveniuc, Stefan, John Kelsey, and Eugen Leontie. "On the privacy threats of electronic poll books." In *Proceedings of the International Conference on Security and Cryptography*, pp. 281-286. IEEE, 2011.
- Quesenbery, W., Baumeister, L., & Dawkins, S. (2023). Usability and accessibility of electronic pollbooks. NIST Voting Technology Series: NIST VTS. <https://doi.org/10.6028/NIST.VTS.100-3pt1>
- Raadschelders, J. C., & Lee, K. H. (2011). Trends in the study of public administration: Empirical and qualitative observations from *Public Administration Review*, 2000–2009. *Public administration review*, 71(1), 19-33.

- Ryan, Peter Y.A., Steve Schneider, and Vanessa Teague. 2015. “End-to-End Verifiability in Voting Systems: from Theory to Practice.” *IEEE Security & Privacy* 13(3): 59-62.
- Schwarzmann, Alexander. (2021). “Towards a Robust Distributed Framework for Election-Day Voter Check-In.” In C. Johnen, E. M. Schiller, and S. Schmid (Eds.), *Stabilization, Safety, and Security of Distributed Systems: 23rd International Symposium, SSS 2021* (pp. 173-193). Springer International Publishing. https://doi.org/10.1007/978-3-030-91081-5_12
- Shvartsman, A., A. Kiayias, L. Michel, and A. Russell. (2010). On the security and integrity issues of optical scan voting systems. In *County of Nassau Board of Elections against State of New York, New York State Board of Elections*, pages 1–23. Supreme Court of the State of New York, County of Nassau, March 19 2010.
- U.S. Election Assistance Commission. 2021. Election Audits Across the United States. Accessed July 24, 2023. https://www.eac.gov/sites/default/files/bestpractices/Election_Audits_Across_the_United_States.pdf.

PRE PRINT