Restoring Trust in Elections

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Alexander Davis

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Pedro A. P. Francisco, Department of Engineering and Society

1 Introduction

Americans' confidence in institutions as a whole is at an all time low, and trust in elections specifically is declining (Rainie & Perrin, 2019). Confidence has continued to decline year after year in spite of incredible progress made in the technologies used in voting systems. If the way people view elections is not aligned with the actual reality of how they are conducted, how can we understand and try to bridge this gap?

To bridge this gap, it is useful to make a distinction between trustworthiness and trust. Trustworthiness refers to how secure an election actually is, while trust is a more psychological concept that refers to how people perceive an election (Stewart, 2022). Trustworthiness could be influenced by any identifiable security measures in a voting system, such as the presence or absence of security cameras, vulnerabilities in software running on voting machines, or the degree to which networks are connected with the internet. Trust can be influenced by all of these things, but it is also more abstract, and therefore harder to identify and address. The factors involved can be wide ranging - research suggests that trust can be influenced by many kinds of demographic factors including race and political affiliation. Greater knowledge about both the electoral process and technology involved in elections is associated with higher levels of trust (Alvarez et al., 2008). While it might not be surprising that people tend to trust things they are familiar with, this does suggest that there are ways to influence how voters view elections.

I conducted a literature review of various studies and solutions focusing on improving voter trust and analyzed this problem using the framework of Value-sensitive Design. I examined the different stakeholders involved using a stakeholder analysis and also used the technique of a value hierarchy to examine how we can better design voting systems. While there have been many technical studies focusing on how we can improve our election infrastructure or new

emerging technologies that can increase security, there are far fewer studies that address the more human side of election security and how we can help people feel confident that elections are more secure. This study aims to address that gap in knowledge by analyzing different methods and determining how effective they are at restoring/creating trust. This also seems to be the first study that analyzes this problem through a sociotechnical framework.

While engineers designing voting systems should be in touch with the people who directly participate in elections, there is far too often a disconnect between voters and those responsible for running elections. We must ensure that technology is designed in a way that promotes the values of the people using it.

2. Background and Significance

Elections are the foundation of a democracy. Our government functions in large part on the assumption that fair elections can be used to hold elected officials accountable. Failure of elections can and often does result in a breakdown of government institutions, and it leads to general distrust in institutions and apathy amongst a population, so it is essential to ensure they stay intact (Mauk, 2020). As mentioned earlier, we need to ensure elections are both secure (trustworthy) and perceived to be secure (trusted). Traditionally, it is the job of elections officials as well as engineers to ensure that the technologies and procedures used in elections are functioning properly. Trustworthiness usually falls to American voters, who are both asked to participate in elections as well as have faith in the outcomes of elections. This binary relationship can lead to a disconnect between voters, election officials, and engineers.

Voting in the United States has a long and troubled history. While most of the history is beyond the scope of this paper, it is worth noting that many people have legitimate reasons to be

concerned about the validity and fairness of election systems. Historically, many marginalized groups have faced efforts to restrict voting. Some of these efforts have been outright legal disenfranchisement, but many are more subtle, such as literacy tests implemented in the South. It has always been possible to find ways to limit the accessibility to voting, and even today, techniques such as gerrymandering or voter ID laws can be strategically employed in different areas in order to influence electoral outcomes for political gain (source, maybe birch). Histories of discrimination and disenfranchisement in the United States can lead to voters having suspicions about elections, making it unsurprising that race and other demographic factors can be predictive of trust in elections (Alvarez et al., 2008). Any attempt to restore trust must therefore take into account this history and understand the context of why certain voters may lack trust in American institutions, and account for the fact that at times these systems are deserving of some mistrust.

One difficulty with addressing any problems with election is the division in election administration between state, local, and federal governments. Elections are actually administered by local authorities, but both state and federal governments can pass legislation influencing how elections are run and set standards to be followed. As a result of this disconnect, there is no set standard for officials to follow. Different localities (usually referring to counties) are required to buy their own equipment, meaning different states and even localities may have different voting machines and may run elections in different manners. While this system can have some advantages, such as allowing local governments to account for budget constraints and giving autonomy to choose systems theoretically more tailored to local needs, this leads to an election landscape with no real nationwide standard for how elections are run. (National Conference of State Legislatures, 2025) Secure elections thus require integrity from many vastly different

actors, which can increase the likelihood of something going wrong in the process. This can also make it difficult for the average voter to understand the complexities of elections, as many competing systems make it unclear where they stand.

Voting technology has a history of being a contentious topic during elections. One recent example, which helped start many of today's issues with trust, was the 2000 election (Mauk, 2022). Confusion over voting machines may even have changed the outcome of the 2000 election (Cohn, 2024). This issue has been magnified in recent elections, as many politicians including President Trump have raised baseless claims about voter fraud and concerns about election security. By providing such a large platform for election security concerns, this has become a topic on the minds of many voters, regardless of whether these claims have any basis in truth.

3. Methodology

3.1 Value Sensitive Design

Value Sensitive Design (VSD) is, in short, the idea that technologies are not neutral but instead are inherently laden with values. This means that engineers, whether consciously or unconsciously, always create technologies that are inherently value laden. It is impossible to separate technologies from those that created them, and it is also impossible to separate them from their users. VSD allows us to consider technologies in the context of those who make and use them, as well as the values involved. I believe that this framework is appropriate for this context because it allows us to consider how election systems are viewed by both the engineers that build it and by the voters that use it, and consider where these viewpoints diverge (Friedman & David, 2019).

3.2 Stakeholder Analysis

First, we need to identify the different stakeholders, anyone affected by the technology, in this problem. Stakeholders are any group of people that we can identify as using or being affected by the technology in some distinct way, and may or may not have different values when using the technology. While some people will fit into multiple categories, I will be analyzing how they function when acting as a particular stakeholder.

Voters comprise a very broad group of people, so it can be difficult to make generalizations about them. Voters participate in elections by voting in them, meaning they directly experience the electoral process and are directly impacted by the technology they use. While they may simply cast their own vote, voters can also influence friends and family members by talking about elections and therefore influence other voters. By participating in elections, voters can feel more connected to their community and gain a sense of belonging in society (Clark, 2020). Voting technology thus directly impacts how voters view elections, government, and their place in society. While voters are a diverse group, above all they value trust - people that take the time to participate want reassurances that their participation matters and is counted fairly. Other potentially important values include transparency, accessibility, and privacy.

Election Workers are the people responsible for ensuring that elections proceed smoothly. They are also responsible for communicating with voters and ensuring that voters have faith in the electoral process. While the specific roles of workers can vary, they often work directly with voting equipment and therefore have a much deeper understanding of election systems compared to the average voter. Election officials are affected by the technology involved in this process because their job depends on the technology working properly, and on the electoral process

running correctly. They would generally value equipment that is accessible and easy to use (both for voters and workers) and equipment that is reliable, accurate, and functions correctly.

Elected Officials are people who gain some kind of office as a result of elections. These stakeholders run in elections and are directly affected by the elections, since the outcomes of elections determine their political future. They should generally be familiar with the electoral process, but may or may not have familiarity with voting technologies. These values may depend on the official, but they should most importantly value integrity and public confidence, as these stakeholders depend on the public to buy into the electoral process.

Engineers refers to the people that design and build the technology that allows elections to function. They are responsible for delivering systems that function in a manner that is reliable and accurate. Engineers might value a system that is innovative and technically sound, but they also want to ensure that they can make a useful product that can be sold to localities.

This is certainly not an exhaustive list of the kinds of people that can be affected by elections. Another notable group is **non-voters**, who are indirect stakeholders since they do not use the technology but are still affected by it. You could further break down the kinds of individuals working in elections or people designing voting systems, but these are intended to be broad categories that help us categorize the main ways people participate in elections and use the technology involved.

Value Hierarchy

A Value Hierarchy is a technique that allows us to organize values into categories. This lets us see which values are more aligned with one another and allows us to design requirements for technologies that can satisfy these values. This allows us to take an abstract idea like trust and

turn it into actionable, concrete design requirements that allow us to build technology that can implement these ideas.

4. Literature Review

There has been a lot of discussion recently about misinformation, specifically with the context of misinformation about elections. A poll from July 2023 found that 40% of Americans believe the outcome of the 2020 election was illegitimate (Ecker et. al, 2024). This is an incredibly high number, especially in an age where information is so readily available. While misinformation is certainly nothing new, what separates current misinformation efforts is the use of generative AI. Instead of needing a person to post misinformation online, malicious actors can create chatbots to pollute the internet with false content. Deep fakes can be used to make convincing videos of political candidates and trick people into falsely believing candidates made a certain claim. While it has always been possible to lie about elections, the scale of misinformation possible now is far greater than ever before (Shoaib et. al, 2023). How does this relate to the values of engineers working on building generative AI models? Most of these engineers do not hold "promoting misinformation" as a value, yet technologies can take on values of their own when they are used. Perhaps they see generative AI as a tool that can unlock human creativity and value the ability to create, or perhaps they see the potential for AI to disseminate knowledge and see their technology as promoting truth, rather than harming it. Perhaps the engineers designed the models without any consideration of value, as can too often be the case. Regardless of intent, engineers have to be mindful of the fact that technology takes on values beyond them, and engineers must still take responsibility for the ways technology could be used. Most people using the internet expect that they can trust content they view, but this is rarely reflected in the design of AI models. One potential technical solution would be to devise counter-misinformation

models that can work to flag false content. For generative models, a watermark could be added in the design (something undetectable to humans but machine readable) that could assist in detection (Liu et. al, 2023). While these methods could raise further concerns about what authority determines truth, it seems clear that we should consider the consequences of AI technologies before we rush to make new ones.

Voting machines have been a point of discussion for decades, and while electronic voting machines promise to modernize voting infrastructure, they can often lead to increased security vulnerabilities. One serious concern about older voting machines is the lack of support for voters with disabilities. Accessibility is an important value for many voters, and many machines have been designed to allow, for example, deaf voters to participate in elections more easily. In addition, using electronic voting machines can simplify the process and make voting less stressful (Ulsan, 2002). On the other hand, voting machines such as DREs pose serious security risks. At a recent cybersecurity conference, a team of experts attempted to compromise several widely used voting machines. Essentially every piece of equipment tested was able to be breached, suggesting that these machines leave our infrastructure deeply vulnerable. One machine had a publicly known vulnerability from a decade prior that had not been patched, another machine was compromised using an unchangeable default password (Blaze et al., 2017). By prioritizing certain values, such as a desire to modernize election systems, we can overlook other security concerns.

Yet another weakness of many machines is that they lack a paper trail and fail to provide reliable verifiability of voting results. While machines can be designed with verifiability in mind, and designs do exist and are in use that provide paper backups for voting results, many localities today still lack machines that satisfy these requirements. Not only are many of these machines

insecure, but they also fail to satisfy values of transparency and reliability. This also helps to highlight another important value conflict - weighing important values such as trust and transparency against more pragmatic values such as affordability. Many localities are small, and lack the necessary staff and funding to implement a truly secure election. These localities often need to use outdated equipment for critical systems and forgo recommended security measures. While localities ideally should invest in security cameras and auditing software, for many localities it is infeasible (U.S. Government Accountability Office, 2018). These examples illustrate how different stakeholders, voters and election workers, may prioritize different values, and further that sometimes realizing all of our target values may not be possible.

One potential solution lies in the case of open source voting. Localities are largely responsible for choosing vendors for purchasing voting systems, resulting in much of the hardware and software involved being owned and maintained by third party companies. This again shows where stakeholder values can clash - companies have a financial incentive to obfuscate voting designs, which often conflicts with voters that value transparency. While companies do have an incentive to ensure machines function as intended, the public is entirely reliant on these companies to ensure the security of their machines, something that seems to not be guaranteed. Open source software exists on the principles of transparency and making knowledge available to everyone. One New Hampshire town has experimented with switching to open source voting software, and seen promising results in increasing voter engagement and trust (Mestel, 2024). Any voter with sufficient knowledge can themselves analyze encryption algorithms and security protocols employed by these machines to verify for themselves the legitimacy of the software. This also allows for neutral parties to audit election proceedings more easily. While this kind of technology is designed with the idea of promoting trust, making code more visible can backfire.

While curious voters would have increased access to voting machines, so would malicious actors. Localities would need to trust that any vulnerabilities would be identified and reported before they could be taken advantage of. Beyond potentially exposing code to malicious parties, there is also concern about how effective open source voting machines would actually be. By making these systems more transparent, localities would be implying there is a need for more transparency, and some voters could misinterpret this as a sign of insecure elections. This highlights a common theme with many of these technologies - by designing technology that promotes trust, you also undermine it by implying trust was broken in the first place. Localities need to weigh the potential gain in trust by empowering voters to familiarize themselves with their voting process against the potential harms in trust that keeping election security in the spotlight could cause.

As a final note, we can look at the case of how an emerging encryption technology, homomorphic encryption, has been utilized to increase trust. In brief, homomorphic encryption is a method that allows for mathematical operations to be done on encrypted data without first decrypting it. In voting machines, this can be used to create a mechanism allowing voters to arbitrarily discard their own votes in order to compare the recorded result with their submitted vote, such as the implementation in Microsoft ElectionGuard (Fleming, 2024). This seems like an innovation that can promote all of the values that reasonable voters would desire - by allowing for users to view the results of votes, they can see first hand the authenticity of the voting process, and by letting voters directly engage in the process of safeguarding election security, they can promote personal agency and investiture in the democratic process (Newman, 2021). This is certainly a promising step forward, but it also has a key flaw that becomes apparent when reading the documentation page - who is this actually for? The algorithm is a technically sound,

brilliant innovation, but also not something that the average voter would be able to grasp - certainly not without investing effort into researching the technology. While homomorphic encryption could convince a cybersecurity expert of the validity of an election, these same cybersecurity experts were responsible for designing the system and rarely need to be convinced. When designing systems with values in mind, engineers must be mindful that systems take on values of their own when being used.

5. Results and Discussion

Analyzing several different case studies gives us some insight into how voting technology has shaped voting security and people's perception of security. By studying generative AI, we looked at a technology not made with elections in mind, but with uses and consequences that are very relevant to elections. The consequences of generative AI show that engineers need to design systems with values in mind, so that we can design technologies tailored to the values of the people that use them. By analyzing voting machines, we further saw the consequences of not considering values like trust, how stakeholder values can conflict, and how values can be exclusive, meaning systems we design cannot always satisfy all of the people they serve. By analyzing open source software, we see a potential solution for building trust, but we also see the tradeoffs of only prioritizing that value. By looking at homomorphic encryption, we were able to further expand on this idea and see that merely designing systems for certain values can be insufficient, as we also have to consider values in the context of whose values they are and how users will utilize the technology.

By looking at different technologies that influence elections and how this reflects the values of those involved, we can see some conflicting arguments. How can we design voting machines for

voters when different stakeholders hold conflicting values? One of the main takeaways is that intent matters. Technology can grow in unintended ways when used, but the worst outcomes generally come when engineers treat technology as value neutral, and fail to consider how and for whom they should be designing technology.

For the final part of the VSD framework, we can build these findings into a value hierarchy. The intrinsic value at the top would be trust, as the overarching value that election systems should promote. Intrinsic values, or values that help us achieve trust, would include accessibility, transparency, and accuracy. Voting systems should be designed in ways that not only promote security and functional elections, but in ways that ensure every voter can participate and can feel invested in the process. Design principles (abstract concepts of what technologies should do) would include explaining voting systems to users and ensuring that votes can be verified. Specific design requirements would vary depending on the particular technology used. This is meant to be a general hierarchy that could be more specifically applied to a particular voting machine or technology meant to promote trust.

6. Conclusion

It can be tempting to take a pessimistic view of the problem of restoring trust in elections. A study of voter data found that by far the most predictive measure of a voter's trust in the electoral process was the performance of the voter's political party and candidates of choice in the previous election (Mauk, 2022). If voter "trust" in elections is really just a reflection of how voters feel about elections, can we ever truly restore trust in elections? It is clear that answering this problem requires collaboration - both from the engineers and public workers designing voting systems and the voters using them. While it might never be possible to completely restore

trust, I believe that it is worthwhile to promote trust, and that we can work towards a better election system. By taking a value based approach to designing election systems, we can ensure that all stakeholders have a voice in elections. By connecting voters with the people running elections, we can work towards rebuilding trust without compromising security.

7. Reference list

Ikrissi, G., Mazri, T. (2024). Electronic Voting: Review and Challenges. In: Ben Ahmed, M., Boudhir, A.A., El Meouche, R., Karaş, İ.R. (eds) Innovations in Smart Cities Applications Volume 7. SCA 2023. Lecture Notes in Networks and Systems, vol 906. Springer, Cham. https://doi.org/10.1007/978-3-031-53824-7_11

Wadowski, G. M., Otte, L. S., Bernardo, N. D., & Macht, G. A. (2023). *A comparative study of electronic voting and paper ballot systems in modern elections*. https://www.example.comhttps://esra-conference.org/files/election-science-conference/files/a_comparative_study_of_electronic_voting_and_paper_ballot_systems_in_modern_elections_wadowski_-_uri_club_tennis.pdf

Blaze, M., Braun, J., Hursti, H., Hall, J., MacAlpine, M., & Moss, J. (2017, September). Defcon 25 voting Machine Hacking Village. DEFCON. https://defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

Mauk, M. Electoral integrity matters: How the electoral process conditions the relationship between political losing and political trust. *Qual Quant* **56**, 1709–1728 (2022). https://doi.org/10.1007/s11135-020-01050-1

Alvarez, R. M., Hall, T. E., & Llewellyn, M. H. (2008). Are Americans Confident Their Ballots Are Counted? *The Journal of Politics*, *70*(3), 754–766. doi:10.1017/S0022381608080730

Ecker, U., Roozenbeek, J., van der Linden, S., Tay, L. Q., Cook, J., Oreskes, N., & Lewandowsky, S. (2024). Misinformation poses a bigger threat to democracy than you might think. *Nature*, *630*(29-32). https://doi.org/10.1038/d41586-024-01587-3

Bush, S., & Prather, L. (2023, January 13). How to restore trust in U.S. election results. *Greater Good*. https://greatergood.berkeley.edu/article/item/how_to_restore_trust_in_us_election_results

Stewart, C., III. (2022). Trust in elections. *Daedalus, 151*(4), 234–253. https://doi.org/10.1162/daed_a_01953

Claassen, R.L., Magleby, D.B., Monson, J.Q. et al. Voter Confidence and the Election-Day Voting Experience. Polit Behav 35, 215–235 (2013). https://doi.org/10.1007/s11109-012-9202-4

Mestel, S. (2024). How open source voting machines could boost trust in US elections. *MIT Technology Review*. https://www.technologyreview.com/2024/03/07/1089524/open-source-voting-machines-us-elections/

Rainie, L., & Perrin, A. (2019, July 22). *Key findings about Americans' declining trust in government and each other*. Pew Research Center. https://www.pewresearch.org/short-reads/2019/07/22/key-findings-about-americans-declining-trust-in-government-and-each-other/

Birch, S.: Electoral Malpractice Comparative Politics. Oxford University Press, Oxford (2011)

Friedman, Batya & David G. Hendry (2019). Value Sensitive Design: Shaping Technology with Moral Imagination. MIT Press.

Clark, J. (Ed.). (2020). *Civic engagement for empowerment and belonging*. Othering & Belonging Institute, University of California, Berkeley. Retrieved from https://belonging.berkeley.edu/sites/default/files/civic_engagement_paper_collection.pdf

Liu, A., Pan, L., Hu, X., Li, S., Wen, L., King, I., & Yu, P. S. (2023). *An unforgeable publicly verifiable watermark for large language models*. arXiv. https://arxiv.org/abs/2307.16230

Shoaib, M. R., Wang, Z., Ahvanooey, M. T., & Zhao, J. (2023). *Deepfakes, misinformation, and disinformation in the era of frontier AI, generative AI, and large AI models*. arXiv. https://arxiv.org/abs/2311.17394

Burton, D., & Uslan, M. (2002). *Cast a vote by yourself: A review of accessible voting machines*. American Foundation for the Blind. https://www.afb.org/aw/3/6/14889

U.S. Government Accountability Office. (2018). *Elections: Observations on voting equipment use and replacement* (GAO Publication No. GAO-18-294). https://www.gao.gov/assets/gao-18-294.pdf

Fleming, S. (2020, April 13). *What is homomorphic encryption and how can it help in elections?* Microsoft On the Issues. https://news.microsoft.com/on-the-issues/2020/04/13/what-is-homomorphic-encryption-and-how-can-it-help-in-elections/

Newman, L. H. (2021, June 3). *Microsoft's vote tracking software clears a major hurdle*. WIRED. https://www.wired.com/story/microsoft-hart-electionguard-vote-tracking-software-partnership/

National Conference of State Legislatures. (2025, April 25). *Funding election administration*. Retrieved from https://www.ncsl.org/elections-and-campaigns/funding-election-administration

Cohn, N. (2024, March 30). *Revisiting Florida 2000 and the butterfly effect*. The New York Times. https://www.nytimes.com/2024/03/30/upshot/florida-2000-gore-ballot.html