VOTER PRIVACY: A TRANSATLANTIC COMPARISON OF ELECTORAL SYSTEMS

A Thesis
submitted to the Faculty of the
Graduate School of Arts and Sciences
of Georgetown University
in partial fulfillment of the requirements for the
degree of
Master of Arts
in Communication, Culture, and Technology

By

Catherine Jones Boardman, B.A.

Washington, D.C.
April 22, 2019
VOTER PRIVACY: A TRANSATLANTIC COMPARISON OF ELECTORAL SYSTEMS

Catherine Jones Boardman, B.A.

Thesis Advisor: Meg Leta Jones, Ph.D.

ABSTRACT

Protecting voter privacy in modern democratic elections involves a highly complex sociotechnical system made up of interconnected people, technologies, legal frameworks, political cultures, and procedural practices. Elections in the United States stand out among all other Western democracies not only for their recent controversies, but also for their decentralized system of voting technologies, electoral administrations, and electoral laws. This paper will compare national elections in Estonia, Finland, Spain, and the United Kingdom to expose the strengths and weaknesses of the United States voting system and to show how voter privacy is an integral ingredient to democratic elections. Each of the selected countries implement different structures of electoral authority, utilize different voting technologies, follow different procedures, and operate within different legal frameworks and political cultures. Unlike in European democracies, the experience of voting in the United States differs depending on which state the voter is from. Although the U.S.’s patchwork system of electoral practices obstructs the voting process from adequately and equally protecting voter privacy, the system fits the unique circumstances of the American political system. The goal of this paper is to illustrate how voter privacy is of constitutive and instrumental use to the puzzle that is democracy.
ACKNOWLEDGEMENTS

This thesis would not have been possible without the help and inspiration of Dr. Jones. Working with you on this project has been such an honor. I never thought a first day of class homework assignment would evolve into a one-hundred-page thesis, but here we are! Thank you for forcing me to overcome my fear of emailing strangers, for cold calling us in 505, for constantly encouraging me to think across disciplines, and for opening me up to the world of privacy.

Thank you, Dr. Koliska, not only for being my second reader, but also for pushing me to become a better writer. Each of your classes pushed me to reconsider my conceptions of truth and reality, and to challenge taken-for-granted assumptions. Thank you for your constant encouragement and for inspiring me to think critically and thoughtfully!

To my Mom, thank you for not helping me with my science projects for me when I was a kid. This paper, I hope, shows you it was worth it.

To my Dad, thank you for the long phone calls, for reading every one of my papers, and for encouraging me to read everything and anything.

To my brother and sister, sorry for bringing up elections and voting at every family holiday. I can’t promise I’ll stop, but I love you!

Lastly, thank you to all my family, friends, and everyone at CCT who had to hear me rant about voting machines.

Many thanks,
Catherine Jones Boardman
# Table of Contents

I. Introduction ........................................................................................................... 1

II. Literature Review .......................................................................................... 6

   History of the Secret Ballot ................................................................. 6

   Arguments Against Secrecy in Elections .............................................. 8

   Arguments in Favor of The Secret Ballot ........................................... 9

   A Sociological Perspective .............................................................. 9

   Voter Privacy .................................................................................... 11

   Threats to Voter Privacy ................................................................ 14

   Arguments Against Electronic Voting .......................................... 16

   Postal Voting .................................................................................... 18

   Effects of Electoral Reform ............................................................ 20

   Voting as a System .......................................................................... 23

III. Method ......................................................................................................... 25

   Why Compare Transatlantically .................................................... 26

   Selected Case Studies ................................................................ 28

IV. Analysis ..................................................................................................... 33

   Estonia .............................................................................................. 33

      Context .......................................................................................... 33

      e-Estonia .................................................................................... 33

      i-Voting ...................................................................................... 36
<table>
<thead>
<tr>
<th>Country</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Secrecy</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Legal Framework</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>Election Administration</td>
<td>42</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
<td>44</td>
</tr>
<tr>
<td>Finland</td>
<td>Context</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Election Administration</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td>Legal Framework</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Voting Technologies</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Secrecy</td>
<td>49</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
<td>51</td>
</tr>
<tr>
<td>Spain</td>
<td>Context</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Legal Framework</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>Electoral Management</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Secrecy</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>Voting Technology</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Conclusion</td>
<td>59</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Context</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Legal Framework</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Electoral Commission</td>
<td>62</td>
</tr>
</tbody>
</table>
Secrecy ....................................................................................... 63
Electronic Voting ....................................................................... 66
Conclusion ................................................................................. 68
United States ............................................................................................ 69
Political System .............................................................................. 69
Context................................................................................................. 70
Legal Framework of the United States ...................................... 71
The Secret Ballot in the Law ..................................................... 72
The 2000 United States Presidential Election ......................... 74
Electoral Administrations .......................................................... 76
Voting Technologies .................................................................. 79
The Decentralizing Effect .......................................................... 82
Conclusion ................................................................................. 84
V. Discussion ............................................................................................ 87
Figures............................................................................................................................ 92
References.................................................................................................................... 101
LIST OF FIGURES

Figure 1. Optical Scan Voting Machine ................................................................. 92
Figure 2. Direct Recording Electronic Voting Machine ........................................... 92
Figure 3. Model of a Voting System ..................................................................... 93
Figure 4. Summary of Each Country’s Voting System ......................................... 94
Figure 5. i-Voting in Estonia ................................................................................ 95
Figure 6. Envelope Scheme .................................................................................. 95
Figure 7. The Principle Parties of the i-Voting System ........................................... 96
Figure 8. Finland’s Experiment with Touch Screen Voting Machines .................... 96
Figure 9. Spanish Polling Place ............................................................................ 97
Figure 10. Example of a Ballot Paper in the United Kingdom ............................... 97
Figure 11. Counting Process in the United Kingdom ......................................... 98
Figure 12. The Five Different Kinds of Chads ..................................................... 98
Figure 13. Palm Beach’s 2000 Butterfly Ballot ..................................................... 98
Figure 14. Votomatic Voting Machine Used in the 2000 Election ........................ 99
Figure 15. Patchwork of Voting Technologies Across the United States................. 99
Figure 16. Premier/Diebold AccuVote OS Optical Scan Machine .......................... 100
Figure 17. ES&S’s AutoMARK OS Ballot Marking Device .................................... 100
Figure 18. Comparison of Geography and Population ........................................... 100
I. INTRODUCTION

Imagine if in the next elections, instead of casting your ballot from the privacy of a voting booth, your vote will be made public. After the election, you will be able to search a database to find the ballots of your family, friends, neighbors, colleagues, or even the barista at your local coffee shop; and they can search you. Would you change the way you vote? Would it even stop you from voting at all? For many, the answer is no. However, for others, the privacy of the voting booth and the secret ballot allows them the freedom to voice their political opinions without fear of intimidation or manipulation. The goal of the secret ballot voting method is to protect voter privacy. Voter privacy, in turn, protects the voter’s ability to choose when, how and if they want to disclose their political preferences. Some voice their opinions freely, putting signs in their yard and bumper stickers on their car, but others may feel in the minority of public opinion within their community and decide to conceal their political views. Both decisions come with a unique set of consequences, outside of the polling station. However, from the sanctity of the voting booth, one casts their vote privately, in isolation, away from the immediate influence of others. Conducting an election via secret ballot involves a complex sociotechnical system of interconnected technologies, procedures, and people that must work in coordination to keep voter’s choices anonymous.

Despite its good intentions, the secret ballot can complicate voting systems and our elections. In 2016, voting systems in Europe and the United States were meddled with by foreign actors. Since ballots are secret, it is challenging to measure the success of Russian hackers with tampering with American voting technology. However, their efforts were successful in drawing attention to the problems with certain voting technologies. When analyzing electoral systems, the
voting technologies, methods, administrational structure, political cultures, and all that they produce, cannot be studied in isolation. Voting machines can only protect voter privacy if the producers, manufacturers, programmers, and election officials are following protocols and procedures. In the United States, state and local election administrations decide which voting machine to use and procedures to abide by, not the federal government. Therefore, the decentralized structure of the American electoral system forms not only a patchwork quilt of voting technologies, practices, and administrations but also a patchwork of vulnerabilities and weaknesses, depending on decisions made at the state and local level.

At the time that the Framers of the Constitution debated divisions of power, Americans had just gained their independence from the most centralized form of government: a monarchy. To safeguard the new nation from future centralized tyrannical rule, they allowed states to self-determine their voting system. Since then, technology evolved, amendments passed, and American elections grew into immensely chaotic logistical events that still are governed with little help from the federal government. While other countries have responded to similar changes by establishing centralized election management bodies, electoral laws, and uniformity into their national elections, the United States refrained. As of 2019, the United States is the only modern democracy with neither a central election administrative body nor a uniform electoral law. Moreover, we are the only country who cannot seem to agree upon how we should vote, when we should vote, and what method or technology we should use to do it. This decentralized structure reflects the nuclear gene of the American DNA: the desire to self-govern. Like all freedom, it comes at a price.
The consequence of the decentralized structure is that without support from the federal government, all future election meddling from foreign adversaries will be an asymmetrical fight. For example, how are local election offices supposed to be equipped to protect their voting system from hacking? Take the 2016 election, for example. The Russian government formed an organization whose sole mission was to poke and prod at American elections. In the Report On The Investigation Into Russian Interference In The 2016 Presidential Election, colloquially known as the “Mueller Report,” there is a portion dedicated to describing how Russia targeted state and local government election administrations (2019, p. 50-51). Despite the redactions, a clear narrative emerges. On one side, you have an organization of the Russian government working around the clock to develop sophisticated cyber warfare apparatus, backed by government funding and resources, dedicated facilities and a vast pool of talent to choose from. On the other side, there is, for example, the local election office in Franklin, Tennessee. Now, in addition to making sure ballots get printed, poll workers trained, and registration lists updated, the election office in Franklin is expected to defend against a dedicated and determined nation-state. This would be like asking the local pharmacy to compete against CVS; it is not a fair fight. Even if Russians, North Koreans, or any foreign actor who wishes to meddle in U.S. elections is unsuccessful in actually altering votes, they still can plant a seed of doubt in the minds of the American public, which is detrimental to the legitimacy of our electoral system.

While even foreign meddling may not motivate support in favor of centralizing election administrations, our mindset about elections can be mended to mitigate future risks. We tend to see problems as having a technological solution, but many of the technical problems in the 2016 election came from the last attempt to fix them. The 2000 Presidential Election and the infamous
Bush versus Gore recount wrongfully accused paper ballots as the culprit. In their search for a quick fix, the government slapped on new, unproven technology as a band aid. The real problem was not paper, but the machines and administration that used the paper. The butterfly ballots were a result of poor ballot design and the chads hanging came from old, poorly designed voting devices. Worse, however, is that after the 2016 election many states - like my home state of Georgia - are ‘upgrading’ their voting systems with technology that is proven to be unreliable, insecure, and dangerous to voter privacy. As the saying goes, insanity is doing the same thing over and over again and expecting different results.

The United States voting system is the black sheep in the family of modern Western democracies. To further understand where the United States can improve their electoral system, this paper will analyze how other democracies conduct their national elections. Estonia, Finland, Spain, and the United Kingdom were selected based off of their similarities to the United States and also their differences. Each country has a unique way of protecting their citizens right to a secret ballot and voter privacy. Many argue that exposing the flaws in the American voting system will only further the disenchantment of voters from the democratic system, delegitimize elections, and further depress turnout. Many argue that American elections are too flawed to fix or that Americans are too idealistic and ingrained in their system to listen to how it may be changed. However, to secure future elections and political privacy, we must.

This paper begins by outlining the existing literature on the secret ballot which combines research from sociology, law, political science, computer science, and voting systems. Next, the case will be made for introducing the secret ballot in the realm of privacy scholarship by showing the overlap between privacy theories and the principles and objectives of the secret
ballot. Using Roy Saltman’s (1989) analysis of voting systems as a model, the literature is then applied to discuss the various types of legal frameworks, electoral administrations, voting methods, technologies, and procedural practices exercised in Estonia, Finland, Spain, and the United Kingdom in contrast to the United States. This paper highlights each country’s peculiarities and unique features of their election days, making a case for the importance of history, context, and political cultures in the development of their voting systems. Contextual information largely influences how each country protects voter privacy.
II. LITERATURE REVIEW

Privacy in elections is somewhat of an oxymoron. Voting is a civic and public duty, with implications not just for those within the privacy of your home, but for all in your community. Who one votes for may indirectly affect the lives of many, but it can directly change the lives of those getting elected, giving them power and authority. It is no surprise then that those seeking specific candidates in power may try to influence an individual’s decision making and for this reason, the secret ballot was born. Since the mid-nineteenth century, all Western democracies gradually adopted the secret ballot system. The secret ballot requires that no one can learn how someone voted with or without their cooperation to avoid vote buying, coercion, intimidation, and other consequences that would be detrimental to the democratic process. If the objective of elections is to elect candidates that reflect the will of the people, then the secret ballot assists democracies in striving towards this ideal.

History of the Secret Ballot

The idea of the secret ballot originated in the Roman Republic, but only in the late 19th century would modern democracies begin implementing privacy into their voting systems. In the simplest form, the secret ballot utilizes a paper and pen. Printed on the paper is a list of candidate’s names from which the voter can mark their selection. Without revealing their choice to anyone, the voter folds their ballot and inserts it into a sealed ballot box, which later will be emptied and counted. The secret ballot prevents wandering eyes from peering over the voter’s shoulder using a voting booth. The design of the voting booth, polling station and the ballot itself work together - physically - to make it harder for someone to find out how a voter voted. But, these physical components are not enough to protect the voter’s secrecy; there need to be laws
and procedures as well. Today, all Western democracies have laws, standards, and international covenants stating all elections should be free, fair and held by secret ballot. The secret ballot is so commonplace that it is commonly regarded as the natural complement to universal suffrage and democratic freedom (Crook & Crook, 2011). Significantly, it is the only method of voting endorsed by the United Nations, making it a global norm for democratic elections.

To understand why the secret ballot is essential, we must consider the alternative. Before the secret ballot, elections were held in public places, and the eligible citizen would cast his vote orally in the presence of a judge and his fellow citizens (Jones, 2003). Because one could hear how their fellow citizen voted, politicians, landowners, and wealthy individuals often used their power to influence or intimidate the voter with techniques, such as, blackmailing, vote buying, “cooping” (kidnapping someone to prevent them from voting), and encouraging substantial amounts of drinking (Jones, 2003). These early elections were fraught with violence and corruption, so much so that election day riots often resulted in deaths (Lepore, 2008). However, there were some logistical benefits to public voting. On the one hand, oral ballots allowed for complete transparency and integrity that the votes were counted correctly.

On the other hand, the lack of a physical paper ballot made conducting a recount near impossible, as there was no physical record to recount other than the tabulator’s handwriting. As suffrage expanded and populations grew, the necessity for recounts led to the use of paper ballots. In the United States, partisan newspapers would print ballots with a list of their party’s candidates, which the voter took with them to their local polling station. Often, political parties took advantage of this system by producing separate ballots to identify who voted for their party, implementing a new scheme of vote buying and selling (Fitzgerald, Smith & Goodman, 2017).
Other problems surfaced as election officials began creating ballot boxes designed for stuffing votes and since the system still lacked anonymity, voters could still be bought, blackmailed, and suppressed.

**Arguments Against Secrecy in Elections**

The secret ballot sparked an international debate between intellectuals, politicians, and voters about anonymity, constitutional duties, human rights, and the voting process. Although commonly thought to be a product of Australia, the genesis of the secret ballot was indeed a transnational effort (Crook & Crook, 2011). From the Chartists demands in England to antebellum America, activist movements started an international dialogue among the political elite about how their citizens should vote (Markoff, 1999). The arguments against the secret ballot and anonymity in democratic elections are plentiful. Aristotle argued that judging the character of the speaker is a vital part of public deliberation in his crucial for rhetorical theory (Enos, 1991). Without the identity of the speaker linked to his rhetoric, the public could not effectively deliberate. John Stuart Mill, famously made a case against anonymity in voting, as he believed publicity increases the individual’s allegiance and accountability to their community (Sturgis, 2005). Alternatively, Jean-Paul Sartre argued that the secret ballot encourages citizens to make selfish decisions, instead of thinking about their community (Theuns, 2017). More recently, contemporary political theorists Geoffrey Brennan and Philip Pettit (1990) called for an ‘unveiling’ of the vote because with open or public voting, “citizens are publicly answerable for their electoral choices and will be encouraged thereby to vote in a discursively defensible manner” (p. 311). Each is arguing for what Engelen and Nys (2013) view as the strength of the public ballot: protection of deliberative democracy by requiring one to defend their choice.
Arguments in Favor of The Secret Ballot

Those in favor of the reform regarded “the change as a democratic one, lessening the control of the upper classes over the electorate, and enhancing the voters' effective freedom of choice” (Yakobson, 1995, p. 426). Others in favor argued that while democratic theory asserts the distinguishing feature of democracies is collective deliberation, the secret ballot does not take away the ability to deliberate (Gardner, 2011; Cohen, 1998). By definition, deliberation involves a social activity; however, anonymous speech can also facilitate communication of dissenting ideas. For example, writing under pseudonyms allowed the spreading of political ideas in The Federalist Papers during the Colonial Period, just as it protects anonymous sources in newspapers today. The secret ballot allows voters the same protection. Without taking away one’s ability to deliberate, secrecy protects one’s right to vote while allowing anyone the ability to “share in collectively binding decisions without having to bare their souls to anyone who asks” (Lever, 2015, p. 175).

A Sociological Perspective

On both sides of the argument, the secret ballot has sociological implications; therefore, theories of social conformity and norms can help explain how the absence of a secret ballot could cause a narrowing of individual opinions. According to Elisabeth Noelle-Neumann’s (1974) spiral of silence theory, if one perceives themselves to be in the minority of public opinion, they may self-silence or censor out of fear of social isolation, unpopularity, punishment, and social exclusion (Steen-Johansen & Enjolras, 2016; Sowell, 1992). Social conformity can have societal consequences as well. As Hayes (2007) describes:

On the one hand, failing to speak unpopular opinions can facilitate the downward spiraling of certain perspectives in spite of them being relatively common in the distribution of public opinion—something that is difficult to construe as healthy for the public good. On another hand, keeping disagreement to oneself helps
to maintain social harmony and the positive face of one’s interaction partners while simultaneously minimizing the likelihood of negative evaluation by those partners (p. 786).

The secret ballot protects those who are in the minority (and majority) of opinion by allowing voters to express their real political ideologies by voting for their candidate of choice, without the uncertainty of revealing any private information (Karpowitz et al., 2011; Brandt & Sandholm, 2005). With the secret ballot, we create a “quasi-statistical picture” of the majority opinion (Noelle-Neumann, 1974, p. 44), but anonymity allows us the freedom to choose when we wish to speak unpopular opinions. Without secret ballots, the idea that one’s friends, family, and employers may cause one to conform to mainstream ideas, or it may stop them from voting at all.

Leading up to elections, people may feel socially obligated to discuss their choice of candidate and other political views, especially in the American political culture of buttons, bumper stickers, and yard signs (Gerber et al., 2013). While many believe that voter intimidation, threats, and other violent tactics no longer takes place in modern democratic societies (Theuns, 2017; Brennan & Pettit, 1990; Engelen & Nys, 2013; Sturgis, 2005; Gardner, 2013), open voting could harm one’s financial well-being. For example, an employee would have to weigh the economic costs and benefits of potentially losing their job if their vote did not align with the company’s principles. It could even take less drastic effects, such as winning or losing a promotion, being assigned to favorable or undesirable shifts, or other workplace punishments and rewards (Gerber et al., 2013). In February 2009, The New York Times reported that some donors to same sex-marriage groups received death threats, envelopes with suspicious substances, and their businesses were boycotted (Stone, 2009). If these donations were secret,
maybe some of these instances could have been avoided, and these situations are precisely what the modern secret ballot prevents.

**Voter Privacy**

The goal of the secret ballot is therefore to achieve political privacy for the voter. Despite the overlaps between privacy theories and the principles of the secret ballot, voter privacy rarely enters into the realm of privacy scholarship. Among privacy scholarships, a consensus has not been reached as to what privacy is and entails, but most seem to agree with Allen’s (2005) analysis that privacy includes:

1. freedom from government or outside interference with personal life—decisional privacy;
2. seclusion, solitude, and bodily integrity—physical privacy;
3. confidentiality, anonymity, data protection, and secrecy of facts about persons—informational privacy; and
4. limits on the use of a person’s name, likeness, identity, or other attributes of identity and exclusive possession—proprietary privacy (p. 485).

Sturgis (2005), one of the few who grapples with privacy and the secret ballot, argues that the secret ballot does not fall within the realm of privacy because “the etymological roots of privacy refer to that which is independent of civic life” (p. 18). However, the secret ballot fulfills Allen’s (1987) description of privacy which can include both "conditions of restricted access," ranging from anonymity, physical separation and information nondisclosure, and "freedom from governmental or other outside interference with decision making and conduct, especially respecting appropriately private affairs" (p. 461, 464-466). Similarly, Westin (1967) argues that privacy is a relationship between the individual and society that takes on four primary states: solitude, intimacy, anonymity, and reserve. Voter privacy requires solitude or freedom from the observation of others; it allows voters to discuss their choice in intimate situations, but they can also reserve or hold back elements of their personality. Lastly, votes are published anonymously in the form of election results.
The secret ballot gives voters privacy in the form of control over information about themselves (Fried, 1968). In this understanding, the choice is whether to grant or deny access to information, both in quantity and quality, similar to Gavinson’s (1980) argument that privacy is a form of limited access to the self. To vote, we leave the realm of the private as we travel to the polling station. Within the voting booth, the voter is not only granted a private space but also anonymity and freedom of thought as Brettschneider (2007) describes:

In deciding how to vote, citizens are entitled to freedom from coercion and to a “private space” in which to make up their own minds through the exercise of political judgment. The privacy of the voting booth serves to enhance this sense that we are free to make our own decisions without external coercion. This rationale also extends beyond procedural protections in the paradigmatic case of voting to the general role privacy rights play in a citizen’s capacity to think of themselves as rulers (p. 75).

Somewhat paradoxically, election officials and the state must coerce privacy to prevent voter coercion. Anita Allen (1999) makes a case for coercing privacy because most individuals surrender their privacy regularly. With the secret ballot, the state creates what Buchstein (2004) calls “auto-paternalism” which is a method of binding all autonomous citizens to prevent situations of corruption, coercion or undue influence (p. 53). Usually the state forcing anything upon its citizens in a democratic society is seen negatively, but voter privacy protects the individual and the collective in a democratic society.

To maintain democratic order, both deliberative democracy and individual capacity for self-determination are required (Schwartz, 1999). On the one hand, the secret ballot allows voters the choice to voice their opinion and deliberate if they choose. The secret ballot is often framed as protecting individuals from harm, but as Priscilla Regan (1995) argues, privacy is also a collective value. She believes that we should shift the conversation from thinking about an individual claim to a social claim because privacy is of public benefit to all individuals in a democratic system (Regan, 1995). Democracy requires publicity, but it also requires secrecy and
privacy (Thompson, 1999). Just as the government must keep secrets to protect national security, the confidentiality of the ballot protects not only individual voter privacy, but it also protects our electoral system from harm.

On the other hand, the secret ballot protects an individual's need for informational privacy on the road to self-discovery. The ability to think privately affords the individual time to self-reflect and develop the skills needed to resist the social pressures of conformity (Rouvroy & Poullet, 2009). Julie Cohen (2000) argues that privacy’s purpose is to promote the development of autonomous individuals and civil society, steering us away from the mainstream and allowing us to aspire towards individuality. Shielding one’s ballot from the public eye secures the individual’s ability to communicate and participate and; to test out different personalities as we develop our own (Simitis, 1987). Voter privacy protects our individuality, personhood, and identity by separating the self from being judged in the public arena by our candidate choice. In a world in which information can easily be judged out of context (Rosen, 2000), our political privacy can prevent others from making inaccurate assumptions about our character, motivations, and values based on our political choices.

In sum, privacy theories and the principles of the secret ballot align in regards to control over personal information and freedom from governmental interference or outside influence into our decision making. The formation of vote preferences will take place in a social context, and social forces will inevitably influence individual voters. Striving to ensure voter privacy is achieved through the method of the secret ballot (Birch & Watt, 2004). Although voter privacy does not have its place in the privacy literature, many of the ideas about the importance that privacy plays in a democratic system can also extend to the principles of the secret ballot.
Threats to the Voter Privacy

By nature, the secret ballot requires technology to protect voter privacy. Although in the 21st century the ballot box, printed paper ballots, writing utensils, and voting booth are simple technologies, each had to be invented. Modern voting technologies, however, create new challenges not only within the polling station but also outside of election day. Since the 19th century, the mechanism of the secret ballot has evolved as a result of competing needs of timeliness, accuracy, security, verifiability, reliability and of course, secrecy concerns. Hand-counting paper ballots can be time-consuming and easy to make mistakes, so as computers evolved it seemed as though they would provide a natural solution to human error-prone methods of counting votes.

From the computer science perspective, creating such a voting technology is like an algorithm that needs to execute the following tasks:

1. Allow each person to vote once
2. Accurately record and count the votes
3. Allow the voter to be sure their vote is counted, without trusting the other side’s people
4. And to vote secretly - so that no one can learn how a person voted against their will or even with their cooperation. (Appel, 2011).

There has yet to be an electronic voting system that can fulfill each task accurately, securely, reliably, and transparently. Most of the advanced democracies in the world still rely on paper ballots, which may be a testament to the lack of trust and certainty governments have when it comes to computers. Paper ballots are readable, countable (and re-countable by humans), durable, and very difficult to tamper with (Bernhard et al., 2017). Paper ballots are often thought to be the safest voting method because there is no “transmission” of votes over the internet, there is no software, no updates, and no memory cards.
Even though computer scientists repeatedly conduct studies showing the vulnerabilities in electronic voting machines, the United States continues to depend on technology for their elections. Most experts agree that hand-marked paper ballots and optical scan voting machines are the best options (Simons & Jones, 2012; Appel, 2018). Optical scan voting machines resemble a fax machine and act like an SAT scantron. The voter marks their paper ballot in private, inserts the ballot into the device and the ballot is stored in a sealed container. The machine reads the ballot and tabulates the vote count based on the absence or presence of a black circle. This method combines technology’s ability to count accurately, with paper’s affordance of being voter-verifiable, trustworthy, human readable, and recountable.

In contrast, Direct Recording Electronic machines - the second most popular in the United States - do not require any hand-marked paper. DREs work similarly to an ATM in that the voter touches the screen to select candidates. There are two kinds of DREs: ones that produce voter-verifiable receipts and ones that do not. Voter-verified paper audit trails (VVPAT) are paper ballots printed out by the DRE voting machine after votes have been cast. This allows the voter to verify their results using an electronic voting machine, while also implementing paper verification (Schneier, 2004). Although DRE voting machines were seen as a replacement for mechanical lever voting machines, the same problems persist in the newer digital versions (Evans & Paul, 2004). Like the mechanical lever voting machines, one cannot “know” that the DRE machine has been programmed to record their ballot correctly, therefore voters must trust that the device recorded them successfully (Appel, 2016).

---

1 See Figure 1. Optical Scan Voting Machine.
2 See Figure 2. Direct Recording Electronic Voting Machine.
Many advocacy groups, such as, Verified Voting, The Brennan Center for Justice, and The Center for American Progress, support hand-marked paper ballots and vehemently oppose DRE machines without VVPAT because of the apparent security threats. Mercuri et al. (2002) and Neumann et al. (1993) both argue in favor of hybrid systems that use electronic voting machines (DRE) and paper receipts. Shamos (1993) connects the dots between secrecy and auditability as he argues:

Even if the voter could be given a receipt, which we have seen is impermissible, what good would that do? Through error, the receipt might be correct, but the vote might still be recorded erroneously. But what if there were independent mechanisms, one at the point of capture and one at the end of recording, both of which produced receipts and these were compared for verification before the vote was permanently registered? This may reassure us against an innocent programming error, but it does not protect against deliberate tampering with the equipment. It is, therefore, wrong to point to anonymity as the enemy of auditability (p. 3).

Because the VVPAT provides a physical record, this ‘feature’ presents new uncertainties for the secrecy of the ballot. At the most basic level, the need for verification that one’s ballot was cast correctly conflicts with voter privacy because verification implies one can prove how they voted (Bernhard et al., 2017, p. 1). This debate sheds light on how modernizing election technologies to solve one problem can also generate problems in other areas such as security, verifiability, and secrecy of elections. To avoid potential threats to voter privacy the obvious solution is to revert to hand-marked paper ballots, just as many European nations have done after piloting electronic voting machines.

**Arguments Against Electronic Voting**

Overall, there are three core arguments in the debate against using electronic voting mechanisms. The first is the lack of security. Many argue that since we trust computers and technology with their finances, personal information, and personal communication, that should be able to trust technology to conduct elections securely (Shamos, 1993). Simons and Jones (2012) highlight that just because one has confidence in an ATM with their finances does not
necessarily mean that a DRE voting machine should be trusted. In a 2018 study by The Center for American Progress, researchers found that hacking and introducing malware on electronic voting machines is straightforward, especially in the 42 states use decade-old software (Root, Kennedy, Sozan & Parshall, 2018). Which brings us to the second criticism of electronic voting machines, the reliability and longevity of the technology. Eventually, all technology renders itself obsolete, and voting technology is no different. Even if someone invented a voting machine that executed every need within a voting system, it would still require maintenance and proper care during storage. Even different models of ballot boxes had to be replaced (Jones, 2001). Lastly, the third argument against electronic voting is that when these machines have to be replaced, it takes a toll on those who will use it. New voting machines require additional training for election officials, and even with proper training, election officials are not expected to be computer scientists or cybersecurity experts and cannot be expected to be able to solve machine failure problems (Schneier, 2004; Lin & Espinoza, 2007). Furthermore, voters have to learn how to use the machines, and without proper education, the experience of voting may be filled with uncertainty as to whether their ballot was cast or not.

Technology can solve human-related issues, but it also obfuscates elements of the voting system into niche areas of expertise. Implementing technology into voting “black boxes” the process from relevant stakeholders: voters, election officials, candidates, and policymakers. This black box effect is problematic for two reasons. First, we cannot see the software programmed into our devices; therefore, we must choose to trust that whoever wrote the code did so accurately. In election technology, this means we no longer need to trust the election officials to count the votes, but instead the responsibility of producing accurate results is in the hands of the
programmer. Second, even for those who can read the programming language, the code programmed into voting machines is kept secret for the sake of securing elections.

The invisible nature of software in voting machines and the lack of transparency has sparked numerous debates. Barbara Simons (2004) argues the software should be made public so that more people could analyze it for bug detection. However, Andrew Appel (2016) explains this would be irrelevant because even if the software is made public, no one can be certain that it is the same software uploaded onto the machine before election day. The software that tallies votes runs on computers and software can be corrupted, and since it has to be updated each year with candidate’s names, it is opened up to what Appel (2016) calls the “fatal flaw of electronic machines.” By this, he means whoever programs the computer decides what election results are reported by the program inside the voting machine. With older machines, a hacker would have to do so manually, but the newer machines have computerized screens, so ‘a bad seed’ could hack the software remotely, or intercept the election results as they are being sent to the central tabulator. Therefore, any voting technology that uses software suffers from the “black box” effect. As Ken Thompson (1984) succinctly put it, “you can’t trust code that you did not totally create yourself” (p. 763).

Postal Voting

The debates over the accuracy, security, and auditability, while important, have sidelined another trend: the gradual erosion of the secret ballot (Felton, 2006) and voting by mail epitomizes this gradual loss of voter privacy. In an attempt to make voting more convenient and increase turnout, many countries in the United States and the European Union began allowing these hand-marked paper ballots to be sent via postal services. This is referred to as remote
voting or voting that takes place outside of the poll site. Polling stations implement voter privacy by design of the voting booth - with curtains, plastic dividers, and privacy slips - and through the presence and supervision of election officials. Without the regulation embedded in the polling place practices, how can we know if the voter marked their ballot in private? Computer scientist Dr. Andrew Appel (2018) argues that even though the postal ballot protocols encourage the secrecy of the ballot, without control of the environment, there is no guarantee that the voter is not coerced, bought, or intimidated. Paradoxically, secrecy in elections is brought about by supervision of election officials (Pratchett & Wingfield, 2004). Therefore, any form of remote voting, whether it be voting over the internet or through the postal system, is inherently incompatible with the principles of the secret ballot (Birch & Watt, 2004).

Within the context of one’s home, Birch and Watt (2004) argue that undue influence is more likely to come from emotion, rather than money or brute force. Even though physical or financial pressures take place while voting remotely, the psychological pressures are “subtle and more difficult to identify, [and] emotional coercion may pose just as serious a threat to democracy” (Birch & Watt, 2004, p. 60). The communal domestic context of the home embodies a far different set of circumstances than the polling station. Families are governed by their own social norms within the privacy of their home which are distinct from norms in the public sphere (Birch & Watt, 2004). For example, voting at home may cause one to think in terms of their honoring their parents rather than being a good citizen. There is no special treatment of upper-class citizens in the protected and controlled domain of the voting booth; everyone is equal. Therefore, it is when voters perceive their vote to be secret and fair that they will be most likely to act independently.
Effects of Electoral Reform

Political scientists have long questioned how specific electoral reforms affect the voting system. While some argue that the secret ballot caused behavioral changes, thereby influencing voter participation (Burnham, 1965), others say that the shift in turnout stemmed from legal and institutional reforms with the introduction of the secret ballot (Rusk, 1970). Cox and Kousser (1981) tested each of their theories through a systematic analysis of election-related stories in newspapers. Their findings suggest that the legal and institutional changes in introducing the secret ballot resulted in a shift in voter behavior. Without being able to buy votes, political parties found new methods of coercion, like paying voters to stay home (Cox & Kousser, 1981). Cox and Kousser’s (1981) study illuminates the complexity of coming to conclusions on what influences voter turnout. Nichter (2008) takes a broader approach by empirically testing whether rewarding and mobilizing voters - “turnout buying” - offers a solution to the secret ballot puzzle (p. 19). With turnout buying, parties monitor whether an individual voted (which is a matter of public record) and offer some reward after. Countries like Australia eliminated turnout buying by making voting mandatory, fining citizens if they do not cast their ballot.

Introducing electoral reforms, whether it be non-optional voting or new voting technologies, can have unintended outcomes. In a national study by Moretti and Card (2006), they looked at whether the introduction of new voting technology affected the outcome of elections. Looking at the 2000 and 2004 United States presidential elections, they found a positive correlation between the use of touch-screen voting (DRE) machines and the level of electoral support for George Bush. Also, they found DRE voting machines harmed turnout rates. In Moretti and Card’s (2006) study, like much of the socio-technical research, the secret ballot is
not at the forefront. Another emerging technology that threatens voter privacy is using biometrics as a form of identification (Hof, 2004). Linking one’s fingerprint, retina, or entire face to a ballot has severe consequences for the secret ballot. Hof (2004) points out the improbability of this ever taking root because “each and every vote has to be linked to a person while preserving the person’s anonymity of what exactly he/she voted for” (p. 70). Even new technologies unrelated to the voting process can pose a threat to the secret ballot, such as with mobile devices and “ballot selfies” (Ohlheiser, 2016). In the United States and Europe, laws are being passed to protect against the risk of revealing one’s identity in “ballot selfies” and the risk of absentee ballots (NCLS, 2017).

Berger, Meredith, and Wheeler (2008) looked into how the location of the polling site influences voters’ choices using priming theory. For example, if the polling site was located at a school, the environment could activate an association cognitively for the individual bringing forward school-relevant norms and causing them to vote in favor of public education. While they did find a correlation between location and cognitive priming, many have found that “there has not been enough emphasis on the internal validity of the political priming effect” (Roskos-Ewoldsen, Roskos-Ewoldsen & Carpentier, 2009, p. 88). In 1992, the Supreme Court upheld in Burson v. Freeman a Tennessee statute that prohibited campaigning within 100 feet of a polling place (504 U.S. 191). Favoring the right to vote freely and without external influences over the First Amendment surprised many, but it shows how sacred the polling place should be. The implementation of the secret ballot, the location of the poll site, the environment surrounding the polling station, and new digital technologies are all factors that affect the election process and can influence the outcome of results.
Government officials often argue that revealing vulnerabilities in a voting system will cause a disenchantment of the voting process, whether real or perceived. However, not pointing out the weaknesses could have more detrimental consequences to the trust voters have in the electoral system. Svedin, Hall & Luedtke (2010) analyze how public fears about risk are filtered through political systems and subjective lenses of perception and how the governments in Europe and the United States are pressured to protect their citizens against these risks. Some argue that technology can increase the level of trust voters have in the voting process (Tapscott, 2018). However, elections get their legitimacy from public trust in the system, not the technology alone. What is most important is that the public perceives elections to be legitimate and they must believe their ballots are cast accurately, securely, and secretly. When one psychologically sees their vote to be secret, it allows voters to express their genuine opinions without fear of personal repercussions (Rusk, 1970). For voters to perceive that their ballot is secret, they must also believe the election administration, voting method or technology, and procedures are functioning accordingly. In summary, democratic elections not only require the voting system to operate in reality, but society must psychologically believe the system is working and that their ballots are kept secret.

Evans and Paul (2004) argue that voting technologies impact both the actual and perceived security of elections. Voters must rely on trust no matter the voting protocol. With paper ballots, there is a possibility that the election officials do not count them correctly and with mail-in votes, the postman and postal service must be trusted as well. With the DRE, the voting interface must be trusted so that the name the voter touches on the screen corresponds with the candidate’s name. Highlighting the common fallacy voters make, Evans and Paul (2004) write
that voters may trust the DRE because of its similarities to an ATM. We must trust the results on
election day without evidence of how everyone else voted. Many believe cryptography to be the
solution to securing elections; however, Van de Graaf (2017) shows that even though using
cryptography could be a secure way to ensure voter verifiable and political privacy in the short-
term, but in the long-term, the possibility of revealing one’s vote threatens the secrecy of the
ballot. With these proposed voting protocols, voters not only have to trust that their ballot will
not be published after election day, but they would have to blindly trust that it will not be
revealed in fifty years.

**Voting as a System**

In 1989, computer scientist and election expert Roy Saltman answered election officials’
questions in regards to electronic voting at the Annual Conference of International Association
of Clerks, Recorders, Election Officials and Treasurers. Election officials asked him how one
could “rig” an election through the voting machines to which Saltman responded:

> Election administration is a system that consists of four elements: (1) people, (2) established procedures, (3)
devices and machines, and (4) activities actually carried out. Activities should be undertaken according to
the established procedures, by people using the devices and machines. Before there were computers, there
were other devices and machines used in election administration, and consequently, some procedures were
different. However, the election process was a system then; it remains a system now. The use of computers
has not changed that. The process remains a system that is managed and carried out by people, that is,
election administrators. The administrators, not vendors, not manufacturers, not other contractors, are
responsible for the accuracy of the results produced. Accuracy must assure that, in the words of the
Declaration of Independence, the Government's "just powers" are derived from the "consent of the governed."
(p. 2).

Saltman accurately argues that we must think of voting as a system. If election officials, voters,
and candidates do not follow the procedures, legislation, and practices in place, then the security
of the voting machines is irrelevant. How elections are run, who is running them, what devices or
methods are they using, what legal framework is in place are all parts of the voting system.

Using Saltman’s analysis as a model through which to analyze national elections in Estonia,
Finland, Spain, the United Kingdom, and the United States, this paper adds historical context as an essential factor to the voting system. Background helps answer why a given country adopted certain voting traits and why others did not.

---

3 See Figure 3. Model of a Voting System.
III. Method

Modern elections are highly complex sociotechnical systems conducted at local, state, national, and even supranational levels. Flawed elections can diminish the legitimacy of any democracy, and since there has yet to be an entirely secure, reliable, verifiable, and secret voting system, all democracies are united in this common struggle. Society, technology, political, legal and procedural systems are all required in the coordination of a voting system. In comparison to other democracies, the voting system of the United States stands out in its approach of holding free and fair elections. Only by comparing voting systems in other Western democracies can one notice these peculiarities. An electoral system will never be able to perfectly protect voter privacy or conduct 100% free and fair elections; however, there are ways for administrations to mitigate risks. The goal of this paper is to compare how different democracies implement voter privacy in their electoral systems to deepen our understanding of how to minimize those risks.

Since there is no voting mechanism in existence that protects voter privacy with absolute certainty, we must think of the secret ballot as a model. All Western democracies agree upon the value of the secret ballot, as it is enshrined not only in national and state constitutions but also in international laws and standards. However, the method for protecting voter privacy varies from country to country, creating a unique lens through which to compare the strengths and weaknesses of modern democratic elections. This paper incorporates research from political science, computer science, sociology, cybersecurity and law to contribute to the existing literature on privacy and the emerging concept of voter privacy. By comparing the voting systems between member states of the European Union and the United States, the analysis will
show how different governments protect the privacy of voters through the organization of their elections.

Why Compare Transatlantically?

Considering the variability in voting methods in the United States alone, one could conduct an interstate comparative analysis; however, these findings would lean towards an ethnocentric view. Instead, the comparative analysis will be across international borders to render the “invisible visible” (Blumler & Gurevitch, 1975) and offer new perspectives on how modern democracies implement voter privacy. As Sartori (2016) eloquently writes, “comparing is ‘learning’ from the experience of others and, conversely, that he who knows only one country knows none” (p. 245). Therefore, through comparative work, we can gain explanations not only about another culture but also about our own. For this reason, the analysis begins with European countries to help reflect on the political culture in the United States.

Sartori (1991) emphasizes that different entities are always and only comparable with respect to the traits they share. For this reason, I chose to compare the United States and member states of the European Union. While both entities are characterized by their freedom of movement, a single currency, and democratic ideals, the United States and the European Union both have many political, economic and social similarities as well as differences. In a comparative analysis by Sergio Fabbrini (2007), he argues that while the United States and European Union may be different ‘species,’ both are compound democracies and are differentiated by the union of states and their citizens. This union requires a delegation of state sovereignty to a higher, supranational or supra-state framework. The inception of both unions came from the necessity to avoid war, but over time evolved into a different kind of political
system. Fabbrini (2007) argues that both the European Union and the United States monopolize the decision-making power through institutions and over time, the process of regional integration in Europe has reduced the historical differences on both sides of the Atlantic. While this may be true, political cultures only apply to the citizens embedded into them, and one core distinction must be made about the founding of both unions. In the European Union, nationality preceded democracy, unlike the United States, “where nationality was the product of the democratic process, not its precondition” (Innerarity, 2014, p. 9). Despite this fundamental difference, on both sides of the Atlantic, there is a tension between those who value the supra-state or supranational entities and there are those who advocate for self-governance, and this tension manifests itself in distinctly unique ways in the European Union and the United States.

Both United States and European Union member states delegate part of their individual ‘state’ sovereignty to a higher power that transcends territorial boundaries. Like the European Union’s member states, there are federal responsibilities, and state responsibilities and both believe that conducting elections is the responsibility of the state. However, while voting systems in the European Union vary from country to country, in the United States, voting systems vary county to county. The lack of national unity in the United States will become apparent in my analysis of election management bodies (EMBs). In the United States, elected officials are in charge of running elections, resulting in high levels of decentralization and partisanship as each county and state has a different way of delegating the responsibility. In contrast, member states of the European Union have independent election management bodies that are responsible for overseeing and conducting elections. I have selected four countries to use as case studies in comparison to the United States because of their relevant similarities and differences.
Selected Case Studies

I selected Estonia, Finland, Spain, and the United Kingdom to compare to the United States due to their varying levels of secrecy practices. Each will serve as a case study through which their commonalities and differences to voting in the United States are comparable. Estonia is similar to the United States in their use of voting technology but stands out in its legal framework for ensuring voter privacy in remote voting. Finland, in contrast, requires all voting to be in the presence of an election official, strictly adheres to paper ballots, and enforces mandatory secrecy. Alternatively, Spain uses paper, but voters do not follow any strict abidance of voter privacy. After elections, however, ballots are burned to erase any trace of voter’s choices. Although the United Kingdom is in the process of leaving the European Union, it is a crucial case to explore because of their approach to evaluating voting technology, a practice that if implemented in the United States could significantly enhance the security of our elections. Furthermore, the United Kingdom, like Spain and Finland, uses no voting technology in national elections, but their paper-based, vote-tracing method could have serious consequences for voter privacy.

Every country transplants certain electoral principles and practices from other countries, but how those practices evolve and are implemented in the voting systems depends on historical context and circumstances. For this reason, no two voting systems are precisely the same, even if they agree upon the same standards. In the United States, transplanting voting systems happens on a regional level. Crook and Crook’s (2011) analysis of the evolution of the secret ballot describes this phenomenon. For example, when other countries were reforming their elections to incorporate the secret ballot, the French government claimed their elections were the most
civilized in the world. That was, however, until they sent election observers to the United States, England, and Belgium and realized the need for secrecy in elections (Crook & Crook, 2011). In contrast, the American adoption of the secret ballot was “more staggered and uneven, principally because electoral law remained a matter of state, rather than federal, determination” (Crook & Crook, 2011, p. 225). The secret ballot began in Massachusetts as an Australian import, and over time, states mimicked other state’s laws, coming up with their own electoral practices and procedures along the way.

Crook and Crook’s (2011) study of French, British, and American adoption of the secret ballot presents a dichotomy between the European and the American way of election reform. The French and English learned from comparing voting systems internationally and reformed their electoral law federally. In comparison to the United States, news of a foreign voting method would either be implemented or influence one state, and other states would follow their electoral reform, but with their own practices. This is true today. European countries carefully pool their knowledge of foreign electoral laws and election reforms to produce a voting system that fits their own unique national character. The United States, in contrast, loosely adopted the ideas of others and innovated upon them in a decentralized, unsystematic way. The American tradition of regular and frequent elections would increase interest in mechanizing the process of voting, making them the only country for much of the 20th century to use electronic voting machines, unlike their transatlantic neighbors. Like Crook and Crook’s (2011) comparative analysis, each country’s unique circumstances will offer historical and contextual information to how their voting systems came to be.
In another relevant comparative analysis, “Two Western Cultures of Privacy: Dignity Versus Liberty,” James Q. Whitman (2004) compares how Europeans and Americans perceive privacy. He argues that American privacy law is “caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity” (Whitman, 2004, p. 1163). The rationale here is that Europeans value privacy as a means to preserve personhood, personal dignity, and reputation, whereas Americans value privacy as a means to ensure freedom from government intrusions. He shows the former through evidence ranging from the laws of dueling and insult to publicizing of nude photographs, paparazzi, and Nazis; the latter is ‘proved’ by examples of Monica Lewinsky, drug testing, and Oliver Sipple. While Whitman’s piece is a compelling cross-cultural read that does offer some insight into privacy cultures, his comparison is not clear. To avoid miscomparing, I will address the same themes for each country.

Each country will be evaluated based on their electoral practices around voter privacy by using reports from the Organization for Security and Co-operation in Europe’s (OSCE) Office for Democratic Institutions and Human Rights (ODIHR). The OSCE is an independent international association that sends election observers to countries all over the world to monitor elections based on the principles of Article 25 of the International Covenant on Civil and Political Rights. The OSCE’s election observers have developed a long-term, comprehensive, consistent, and systematic election observation methodology and they regularly publish detailed reports of their findings. These reports are used throughout the analysis to compare the conduct of elections in each country over many years. Furthermore, the OSCE’s reports offer considerable insight into the three themes I will focus on: administrative structure, voting methods, and legal framework.
In addition to OSCE reports, the Electoral Integrity Project conducted by Pippa Norris and researchers based at Harvard University and the University of Sydney proved extremely useful in quantifying electoral integrity worldwide between the years 2012 to 2017. Measuring fairness in elections is often referred to as electoral integrity. The Global Commission on Elections Democracy and Security defines electoral integrity as “any election that is based on the democratic principles of universal suffrage and political equality as reflected in international standards and agreements, and is professional, impartial, and transparent in its preparation and administration throughout the electoral cycle” (2012, p. 6). Norris adds “perceptions” to electoral integrity “to understand international standards of electoral integrity, what happens when elections fail to meet those standards, and how electoral integrity can be strengthened” (Stedman, 2015). Through surveying hundreds of election experts, Norris ranks the elections of 164 countries using a 100-point scale she created to assess the integrity of any election (Stedman, 2015). The United States ranked the lowest among Western democracies, generating much criticism, partly for equating elections in the U.S. with those in Sierra Leone, Cuba, and Indonesia (Hamze, 2016). However, since then the Electoral Integrity Project adjusted their scale and routinely updates Perceptions of Electoral Integrity. Quantifying electoral integrity is an ambitious goal as election experts cannot physically be at all polling places at once. Each of these sources provides an ample amount of resources and contextual studies with which I will use to compare the integrity of elections in Europe and the United States.

The comparative method approaches a social problem democratically, allowing many voices to be heard and deliberating to find common ground. Comparative analysis asks why is something this and not that. It is an investigation with a goal is to find meaning and to influence
a change. If privacy can be seen as a common good within a democratic society (Regan, 1995),
then how these nations choose to protect the secret ballot through laws, political cultures,
election systems and in the voting technology itself will fill a hole in the research. Throughout
the following analysis, I will provide a brief history and relevant context for each country. Next,
I will cover the themes of voting technology, election administration, legal framework, and voter
privacy. A summary of each country’s context, voting technology, method for protecting voter
privacy, legal framework, and election administration can be found in Figure 4.
IV. Analysis

Estonia

Context

The tiny nation of Estonia, a former Soviet Union satellite state, transformed within a matter of decades into one of the most technologically advanced societies, complete with an entire e-government and e-voting system. To put this transformation in perspective, by the time Estonia defeated Soviet occupation gaining its independence in 1991, most Americans owned personal computers while Estonians still typed on typewriters and called their friends on landlines (DOL, 1999). During the 90s, many countries found themselves approaching a technological fork in the road, asking how new digital technologies would impact the relationship between citizens and governments. The United States chose the path of personalization, information privatization, and profit-maximizing competition, while Estonia decided to unite their nation by building a digital society, one run by a digital government (Heller, 2017).

e-Estonia

Before 1991, there was no digital data being collected about Estonians, as the general population did not have the Internet or even a device to use it. The Estonian government courageously decided to take the information technology route and began developing e-Estonia, a movement dedicated to facilitating communication between the state and its citizens through digital solutions. By 2000, Estonia became the first nation to declare Internet access as a human right. The Riigikogu (Parliament) enacted the Telecommunications Act, which made internet access universally available at a uniform price, regardless of one’s geographical location (Borg,
2011). Joining the European Union and NATO solidified Estonia’s political future, but their technological one would continue to grow. In 2004, Estonia’s penetration rate was 53.6% (10% lower than that of the U.S.), and by 2018, that rate would surpass other well-established democracies, including the U.S. (IDEA, 2018). Prioritizing internet access provided the foundations needed for Estonia’s vision of e-government.

Above all, Estonia’s e-government values convenience. In a few clicks, Estonians can check their bank accounts, access their medical records, view their health care, pay their taxes, ‘sign’ checks, see their school grades, monitor their home’s energy consumption, and vote - from anywhere in the world that has internet connection (Heller, 2017). The key to Estonia’s e-government is the ID card. Almost every Estonian carries with them an identification card, which is just like any other photo ID, except that it has a chip and can be directly inserted into the side of your computer. Unlike the average photo ID, this mandatory digital ID can be used as a proper travel ID for citizens traveling within the European Union. It also grants Estonian citizens access to all e-government services and can be used as a national health insurance card, proof of identification when logging into bank accounts, for digital signatures, to check medical records, submit tax claims, to use e-Prescriptions, and last but not least, to vote.

Using the smart ID card, an individual can authenticate their identity without physical contact. Each Estonian ID card has a unique ID number, which, unlike a Social Security Number does not need to be locked in a safe or shredded after writing it on old documents, because it authenticates the identity using a pin code (Heller, 2017). When an Estonian inserts their ID into a computer and enters their PIN, their data - which they own - is decrypted before their eyes.
Using blockchain technology, the government does not hold personal data on a central server (which prevents Equifax-style security breaches). Instead, Heller (2017) explains:

The government’s data platform, X-Road, links individual servers through end-to-end encrypted pathways, letting information live locally. Your dentist’s practice holds its own data; so does your high school and your bank. When a user requests a piece of information, it is delivered like a boat crossing a canal via locks […]. Beyond X-Road, the backbone of Estonia’s digital security is a blockchain technology called K.S.I. A blockchain is like the digital version of a scarf knitted by your grandmother. She uses one ball of yarn, and the result is continuous. Each stitch depends on the one just before it. It’s impossible to remove part of the fabric, or to substitute a swatch, without leaving some trace: a few telling knots, or a change in the knit.

Rather than guarding your information in one place, personal information lives in bits and pieces, brought to life using a pin code. Heller’s (2017) scarf analogy illustrates the importance of a public ledger, which cannot be breached without leaving a trace because each digital signature has a timestamp.

While this digital utopia seems to have it all figured out, there have been security breaches. The most significant attack took place in February 2007 when hackers temporarily shut down access to banks, media, and government portals, causing chaos throughout the nation (Heller, 2017).Instead of abandoning their high-tech system and retreating to a traditional form of governing, the Estonian government opened a multinational-funded think tank called the Cooperative Cyber Defense Centre of Excellence (CCDCOE) in Tallinn. As a cyber defense hub whose mission is to prevent future security breaches, the CCDCOE’s brings together researchers from all over Europe creating a unique interdisciplinary approach to cyber defense. Overall, the government’s transparency and handling of the 2007 security breach, reaffirmed public trust in the government (Livesay, 2018). Just one month after the 2007 security breach, Estonia would become the first country to use i-Voting in parliamentary elections. While most Estonians went

---

4 The hackers were largely suspected to be Russians, since the breach came after the destruction of a Russian statue in Tallinn, according to Livesay (2018) and Perrigo (2019).
to the polls, 5% of all voters (about 30,000) felt secure enough to use the i-Voting system (Valimised, 2019). By 2017, the percentage of votes cast over the Internet would continue to grow to 31.7% (Valimised, 2019). The increasing number of i-voters is an excellent barometer for measuring the trust Estonian citizens have in their e-government.

**i-Voting**

Internet voting, or i-Voting, is a system that allows voters to cast their ballots from any computer with internet access, from anywhere in the world. Like postal or mail-in voting systems, i-Voting is a form of remote voting in which citizens can cast their ballots from home using a ‘mail-in’ ballot or voting over the internet, instead of physically traveling to the local polling site. Remote voting benefits the military traveling overseas, those with disabilities, the elderly, or those living far from their registered polling by allowing them the ability to partake in their democratic right, despite their personal circumstances. Also, remote voting has been seen as a solution to declining participation and turnout rates (Solvak & Vassil, 2016). Estonians, however, argue the most significant effect of the i-Voting system is its efficiency and convenience. The Estonian government website even claims that “i-Voting saves 11,000 working days per election” (Valimised, 2019). Crucial to the i-Voting system is that i-Voting is just one of many options to participate in the democratic process, as the Estonian National Electoral Committee (NEC) offers four different ways to vote: voting using paper-based methods at the polling site, voting abroad, advance poll site voting and internet voting (i-Voting) (Valimised, 2019).

---

5 See Figure 5. i-Voting in Estonia.
The Estonian government explains how the i-Voting system works by using the analogy of the mail-in ballot (Valimised, 2019). Known as the “envelope scheme,” the mail-in ballot process involves two envelopes. One envelope is for the completed ballot, which has no identifying information about the voter, and once it is sealed, the voter places that envelope into the second one which does have the voter’s information. The envelope is sent to the voter’s polling station, where election officials confirm the voter is eligible to vote. If so, the anonymous inner envelope is put into the ballot box.

Electronically speaking, the voting process looks very different, but from the voter’s perspective, the experience of i-Voting is similar to using any other e-government service. The voter inserts their ID card into the card reader, opens the i-Voting website and downloads a voter application. Next, the voter identifies themselves by entering a pin code and after, a list of candidates in their district appears on the screen. The voter selects their candidate, re-enters their pin code, thereby confirming their “digital signature” similar to signing a mail-in ballot (State Electoral Service of Estonia, 2017). Next, the voter receives a confirmation that their ballot has been accepted. The process is fast, modern, and above all convenient, but on the backend - both on the technical and the administrative side - the process is immensely complicated. For the sake of this paper, it is only necessary to know that the votes are encrypted so that no government official can see how you individually voted. Only the voter can see their own vote choices, just as only they are the only ones who can see their bank statement or energy bill.

---

6 See Figure 6. Envelope Scheme.
7 See Figure 7. The Principle Parties of the i-Voting System.
Secrecy

i-Voting, like any form of remote voting, eliminates the government’s ability to protect the confidentiality of the ballot because, without control of the environment, the voter could be subject to several undue influences. In the polling place, the government delegates the responsibility of making sure every eligible citizen has the right to cast their ballot freely and fairly to election officials. A range of protocols, from the design of the polling place to the use of secrecy sleeves and privacy dividers, ensure that the voter can secretly cast their ballot. When voters choose to vote from remotely, the consequences of public voting resurface. In one’s home, vote buying is unregulated as one can watch someone fill in their ballot and pay them afterward without an election official’s knowledge. In one’s home, voters can be influenced subtly by their spouse or roommate, or forcefully by an intruder. The ability to vote from anywhere with internet access opens the possibility of voting at one’s place of work. Employers could ‘encourage’ their employees to vote together or to vote for the candidate that best supports the company’s agenda. Although many argue that the need for the secret ballot to prevent voter coercion is no longer necessary, there is no way of knowing for sure without surveillance of the voter environment.

There is a common misconception that remote voting is one of the most secret forms of voting since it takes place within the privacy of one’s home. Through Estonian electoral law, it is evident that the government realizes that secrecy cannot be protected in unsupervised environments, and they offer a unique administrative and technical solution to mitigate violations of voter privacy. First, because any form of remote voting cannot ensure that voters are alone or in private while casting their ballot, voters are allowed to change their ballot
electronically and repeatedly during the seven days of advance polling (Solvak & Vassil, 2016). This mechanism prevents a vote buyer or coercer from knowing which ballot will be counted, “rendering vote buying or coercing meaningless” (Solvak & Vassil, 2016, p. 9). One might argue that a coercer can wait until the last minute; however, Estonians anticipated this line of thought and provided the second solution. One of the Estonian National Electoral Committee protocols is the primacy of ballot paper voting, which means “if a voter who has already e-voted goes to the polling station during the advance polls and casts their vote using a paper ballot, then the e-vote is cancelled. After this, the voter cannot recast their vote electronically or using a paper ballot” (Solvak & Vassil, 2016, p. 9). In sum, since remote voting takes place before election day, a voter who believes the secrecy of their ballot was compromised has two options. First, they can recast their vote electronically, as many times as they want, and second, they can choose to go to the polling station on election day and recast their vote, thereby canceling their i-ballot. Estonian voters, therefore, always have the option of secrecy.

While voting digitally using blockchain can help solve secrecy issues, solutions designed to solve security and verifiability concerns create new problems for voter privacy. In response to security concerns, the Estonian National Electoral Committee implemented a system of vote verification that makes it possible for voters to verify whether their vote was cast correctly after the deadline (Solvak & Vassil, 2016). Since there is no paper trail with i-Voting, the verification process requires a smartphone and a voting app. After the voting process, voters can verify their ballots using the app and a QR code (Solvak & Vassil, 2016). Therefore, who is to stop a vote buyer, employer, spouse, or coercer from asking for proof that the person voted how they say they did? Remote voting, thus, presents many difficulties for the secret ballot and internet voting
adds another layer of complexities. Estonian electoral law must be legally flexible to accommodate the future solutions needed to solve new technical issues that will arise. Estonia’s revote system shows how the government already has used this legal flexibility to ensure its citizens can exercise their constitutional right to a secret ballot by offering solutions to possible technical problems.

**Legal Framework**

For any voting reform, there needs to be a legal framework, technological infrastructure, and political culture supportive of the new voting mode (Alvarez, Hall & Trechsel, 2009). The legal framework established in 1992 Estonian Constitution Section 60 reads: “Elections are general, uniform and direct. Voting is secret.” As shown in the previous section and literature review, it is impossible to guarantee secrecy in remote voting. So, to introduce i-Voting into the voting system legally, the Estonian government had to justify the constitutionality of i-Voting. First, the government Estonian used a teleological approach to interpret the Constitution, meaning that the Constitution needs to be “understood through the problems the given principles were meant to solve” (Drechsler, 2003, p. 5). Considering that the Estonian constitution was written at a time when Estonians barely had computers, let alone internet access, the authors of the Constitution had no way of predicting i-Voting or the problems that come with it. Those in favor of i-Voting argued in parliament that since all voters have the right to go to the polling station, then the aim of secrecy is achieved (Drechsler, 2003). Alternatively, the second justification was informed by the Reformierakond ideology (The Reform Party) that argued the government should ‘trust the people’ to do the right thing (Drechsler, 2003). Similar to Allen’s
(2005) decisional privacy theory, the Estonian government believes its citizens should be free from government interference in decision making.

Legal arguments, in Estonia, are always intertwined with the technical. For example, i-Voting would not be possible without the Digital Signature Act that allows for digital authentication of the voter using their ID cards (Alvarez, Hall & Trechsel, 2009). i-Voting requires that a digital signature legally satisfies the need for personal authentication. On a more fundamental level, i-Voting would not have been possible without the Electronic Communications Act (2004), which was responsible for assisting in building the technological infrastructure needed to support Estonia’s e-government. The Riigikogu Election Law was responsible for enacting the “last ballot cast” or revote standard, allowing for voters to change their vote repeatedly or go to the polling station on election day, canceling out their i-ballot (Alvarez, Hall & Trechsel, 2009). Lawmakers must understand the technical components of the i-Voting system to craft effective legislation. Since Estonia is an e-government, one would expect lawmakers to already be well-versed in basic computer science.

This pro-tech political culture allows electoral reforms to happen rather quickly (Alvarez, Hall & Treschel, 2009). Estonia’s unique situation of democratizing during a time when most of the world believed the internet had a democratizing superpower, may explain the culture’s penchant for the digital. However, another factor in Estonia’s political culture is their history as a former member of the USSR. In 1991, the right to vote was a new one. To create a voting system in their new digital democracy, a robust and professional election administration was established: the Estonian National Electoral Committee. Along with the international support gained upon
entrance into the European Union, Estonia had to reach the European Union's democratic standards for elections.

Ever since establishing itself as a democratic e-government, Estonia has welcomed foreign observation into their political culture. In 2015, Estonia invited election officials from the OSCE to observe and evaluate their elections (OSCE, 2015a). Estonia also allowed a small team of American election experts to observe their internet voting method, although it was not evaluated favorably due to security concerns (Springall et al., 2014). In comparison, the United States not only lacks a strong election administration but also does not encourage international election observers. In the United States 2016 election, ODIHR independent election observers were almost arrested in a Texas polling site (Collin, 2016). Estonia’s political culture, however, is not as partisan or ideologically polarized, as in the United States (Alvarez, Hall & Trechsel, 2009). In place of partisan troubles, Estonians have conflicts of ethnicity, a consequence of being occupied by authoritarian regimes. Estonia’s unique circumstances led to their political culture and legal framework to be inexorably intertwined with one another. While there are flaws in their voting system, as no voting system is perfect, Estonia’s dedication to innovation and secrecy is admirable. Estonian law sets a precedent for any other country who will consider i-Voting in their own elections; however, the technological infrastructure and political culture of a nation must be considered, as Estonia’s is exceptionally unique.

**Election Administration**

Estonia’s election administration changes alongside technical, cultural and legal reforms as well. In 2016, Estonia entirely reorganized the distribution of power within local administrations by consolidating the 213 municipalities to just 79 districts, to increase the
efficiency and consistency of local governments (Vahtla, 2017). The Administration Reform Act effectively revisited the ratio of population to authorities, much like the United States reconsiders political districts, but instead of drawing complicated domestic borders, the Estonian government’s goal was to simplify and centralize local authority. The Act consolidated local governments not only to make the most effective government administration but also to streamline the chain of command in conducting elections (Vahtla, 2017).

As of 2019, elections are managed by two structures: The National Election Committee and three levels of election offices headed by the State Electoral Office (OSCE, 2019). Before the reform, there was a middle level of election administration, the 17 County and City Electoral Committees, which now have been abolished to simplify the administration structure further (OSCE, 2019). The National Election Committee is the autonomous institution responsible for the overall management of elections and is composed of five members who are appointed by various branches of government (OSCE, 2019). The Administration Reform Act established the State Electoral Office to oversee the operational preparations and conduct of elections and to work with 79 local election officials and some 550 voting district committees (OSCE, 2019). While the National Election Committee works to ensure that voting occurs within the legal framework, the State Electoral Office focuses on the actual operation of elections, such as the organization of Internet Voting and supervision of the electoral officials (OSCE, 2019). Overall, the Administration Reform Act represents Estonia’s willingness to adapt their electoral administration when needed.
Conclusion

What makes Estonia stand out among Western democracies is not only their progressive i-Voting system but also and more importantly, their ability to change and adapt with their pro-tech political culture. In the 28 years Estonia has been a democratic nation, their government has experienced more technological, legal, and administrative changes than in the 241 years of the United States. While Americans stand firm in their loyalty to the constitution, Estonians swiftly adapt their legal documents to the times and to suit their current needs. While American politicians often use electoral legal reform for partisan gain, Estonians treat elections as a fundamental human right. This could be a result of transitioning from communism to a liberal democracy in the 1990s, which is a far different experience than the United States’ transition from monarchical rule to a democratic republic in the 1770s. Estonia’s voting system works within their small, high-tech political culture, but such a system would not suit the American political system for many reasons. However, how technology influenced the Estonian voting system does in fact mirror that of the United States. Estonia’s legal flexibility and solutions to concerns regarding voter privacy can teach the United States how to craft their electoral law if using voting technologies.

Finland

Context

Like Estonia, Finland’s experience of foreign rulers, alliances, and political culture formed a unique approach to ensuring voter privacy. After seven centuries of Swedish rule and another one hundred years under Russian power, Finland gained its independence in 1917. Unlike their Estonian neighbors who chose to forge a new social and political identity, the Finns
were influenced by their previous Russian and Swedish rulers, resulting in a mix of republican and monarchist ideals (Sjöblom, 2010). Post-World War II, many Western democracies feared Finland would follow Czechoslovakia and become a communist satellite (Sjöblom, 2010). Although capitalism prevailed, Finland had to cope with Soviet pressures, who would continue to influence their foreign and domestic politics. Finnish politicians would have to appeal to Western democracies, while also maintaining good relations with Soviets (Lounasmeri & Kortti, 2018).

The Finnish political landscape struggled to perform this balancing act between Eastern and Western politics. One man President Urho Kekkonen mastered the art of pleasing both the Soviets and Western allies, but it was his authoritarian behavior and interpretation of the constitution that allowed him to remain in power for 25 years (1956-81) (Lounasmeri & Kortti, 2018). President Kekkonen enjoyed immensely broad powers protected by the constitution, which was comprised of monarchist and republican ideas (Lounasmeri & Kortti, 2018). Eventually, Kekkonen’s authoritarianism during his long reign would be the impetus for constitutional reform which took place between 1984 - 2003. These electoral reforms solidified Finland’s constitution and election process to prevent such an overreach of power from happening again. Like their European neighbors, Finland would adopt a parliamentary system with regular free and fair elections (OSCE, 2015b).

Election Administration

The unique circumstances that led Finland to revise its voting system created a stringent and detailed electoral law which is run by a central election administration. Uniform enforcement and application of the election law means elections look the same from municipality to
municipality and national standards trump local and regional authorities (Sjöblom, 2010). The “supreme” election authority in Finland is The Ministry of Justice (MOJ), who oversees all electoral matters (OSCE, 2015b). The MOJ’s primary electoral duties are to provide instructions to lower districts and municipalities, assist them with funding, and conduct voter education projects in the form of advertisements, social media campaigns, and brochures (OSCE, 2015). Starting at the MOJ, the election chain of command trickles down to the local level, which is laid out in Finland’s electoral law. The MOJ routinely assists the 295 municipalities with the cost and administration of elections (OSF, 2017).

In contrast, the United States government has only provided federal funding to local administrations twice in the nation’s history. In the United States, federal election funding is not routine, but often occurs only after an election crisis through the Help America Vote Act (once after 2000 presidential election, and once after 2016 presidential election). These funds are distributed to the states through the Election Assistance Commission (EAC), an independent agency whose purpose other than distributing funds is to provide guidance to states, creates voluntary voting system guidelines, and accredits voting technology (Pastor, 2009). The EAC has no say in how the states run their elections, as the United States Constitution maintains that the responsibility of conducting elections is in the hands of the states. Similarly, Finland’s MOJ cannot enforce protocols on elections, but all local and regional election administrations are enforced through electoral law. In sum, Finland differs from the U.S. in its centralized election authority whose purpose is outlined and clearly stated through the Election Act (OSCE, 2015b).
Legal Framework

At eighty pages long with fourteen chapters, the Election Act of 1998 (amended in 2004) centralizes and unifies the Finnish electoral system. In the United States, any election procedure may vary from one polling station to the next, as there is no federal law or unifying piece of legislation on conducting elections. However, in Finland, their very detailed instructions for how votes are cast and how they are counted leaves very little room for maneuvering in the actual organizing of elections (Setälä & Grönlund, 2004). Every election must follow the following principles that Jääskeläinen (2010) outlines:

- **The elections are direct.**
- **The elections are proportional.**
- **The elections are secret.** Secrecy of the ballot means that neither the election authorities nor anyone else get to know who the voters cast their vote for or whether they returned an empty ballot.
- **The right to vote is universal and equal.**
- **Voting is personal.** The right to vote may not be used through an agent.
- **Voting takes place in front of election authorities.** This aims to guarantee that the elections are trustworthy, the voters may freely express their will, and that secrecy is maintained. The election authorities usually are elected officials (p. 9-10).

Many of these principles are shared throughout the European Union, as they all follow the same international election standards, but the last policy is unique to Finland. Finland takes protecting secrecy to a new level and because of these principles, implementing new voting technologies has been extremely difficult.

Voting Technologies

Finland’s preference for paper-based, traditional voting mechanisms does not mean they are technologically unsophisticated. Finland is extremely technologically advanced. Coming in at number four in the Digital Economy and Society Index (DESI), which measures a nation’s performance across five categories: connectivity, human capital, and digital skills, use of internet services, integration of digital technology in business, and digital public services, across
European nations (DESI, 2018). Similar to the small country of Estonia, Finland belongs to the wired world, as most homes have computer access according to the OECD. Also, Finland also is one of the most digitally competitive countries in the world according to the International Institute for Management Development (IMD, 2018). The MOJ has explored various voting technologies and has similarly issued pilot testing as the United Kingdom. While paper may seem archaic, countries who choose to stick to paper-based voting methods express a greater understanding of technology’s inability to be 100% secure for ensuring free and fair elections.

Like the U.K., Finland has concluded that because the voting technologies available today cannot be 100% secure and cannot 100% protect the secrecy of the ballot, that they are not worth implementing. In 2008, Finland conducted an electronic voting pilot to test a voting machine similar to the DRE touch screen system (Aaltonen, 2015). On election day, voters were given a choice to use electronic voting machines or paper ballots (Aaltonen, 2015). For those who chose to try e-voting, they were given a smart card to enter into the voting machine, and they cast their ballot by typing in the corresponding candidate’s number, confirmed pressing an ‘OK’ button, and then returned the smart card to the election official (Aaltonen, 2015). The testing only took place in polling stations, using electronic ballot boxes and there was no remote voting testing (Aaltonen, 2015). Unlike the DRE machines used in Georgia, the voting terminals were connected to a centralized ballot box, which used an encryption application to send the votes over the internet while protecting the voter’s privacy (Aaltonen, 2015). Because these machines did not produce a voter-verifiable paper trail, voters could only verify their selections on the screen. The lack of verifiability led to a challenge in the court, and the elections were

---

8 See Figure 8. Finland’s Experiment with Touch Screen Voting Machines.
ordered to be redone in the three pilot project municipalities (Goldsmith, 2011). In 2010, Finland
decided to cease development of e-voting at polling stations not only because international
experiences with voting machines tended to be weak, but also because the questions relating to
the secrecy of the ballot remained (Aaltonen, 2015).

The existing voting technologies at the time did not guarantee voting secrecy and were
not wholly reliable; therefore, the Minister concluded that adopting electronic voting was not
necessary (Setälä & Grönlund, 2004). At the time of this paper, Finland still uses paper voting
methods. Finland’s reluctance to implementing election technology is because of its dedication
to maintaining voter secrecy, but outside of elections, Finland is one of the leading countries in
providing public services over the internet (Setälä & Grönlund, 2004). Unlike Estonia, Finland
has rather good reasons for sticking to paper-based methods and old-fashioned techniques at
ensuring voter secrecy. Introducing new technology would require fundamental changes to
Finnish electoral law, administrative and public re-education, and could diminish their electoral
integrity. Without the systemic pressure to introduce computerized or electronic voting, the
Finnish political culture, unlike the Estonian one, mitigates risk through tradition rather than
innovation.

Secrecy

Since all voting must take place in front of election officials, an electoral reform such as
Estonia’s i-Voting would be challenging. Finland considered introducing Estonia-style electronic
identity cards, a vital step in creating the i-Voting infrastructure. However, the Minister of
Justice, Johannes Koskinen, emphasized that the only way of making sure the actual will of the
voter is counted is to monitor the act of voting and protect the secret ballot (Setälä & Grönlund,
Therefore, Finland assumes that the only way to ensure a voter is not coerced, intimidated, or bought is through monitoring of the environment in which the voter performs their secret act. Other voting technologies were trialed and ceased because of the secrecy requirement. While many countries have tried and abandoned electronic voting technologies, Finland’s allegiance to the principle of secrecy is certainly unique and also indicates that electronic elections are probably not in the foreseeable future.

Finland’s mandated secrecy requirement has created a rather strange procedure for postal voting. Similar to the way Estonia found a form of remote voting that works for their political culture, Finland accommodates those who cannot travel to the polling station by allowing postal voting. However, the absentee voter must schedule a time with an election official to go to the voter’s home so they can fill in their absentee ballot under the supervision of an election official. Considering that Finland’s population is almost half the size of that of New York City, requiring an election official be present for filling in of absentee ballots is feasible. However, in the United States, adopting this protocol would be a logistical nightmare and probably would further depress turnout.

Furthermore, the size of the United States makes adopting Finland's system not feasible. Also, the average American may find qualms regarding any election official entering their home for purposes of supervision, as privacy in the United States is primarily considered to protect one from invasions of the home. While privacy is often thought of in terms of physical space in the United States, the Finnish electoral law shows an alternative conception of privacy and secrecy. For the Finns, the protection of the secret ballot is worthy of a momentary invasion of privacy in one’s home. In comparison to other nations in the European Union, the Finns strictly abide by
electoral law requiring the act of voting to take place in the presence of a public official (Setälä & Grönlund, 2004). Therefore, the Finnish government does not rely on trusting its citizens to protect the secrecy of their ballot, but instead they choose to rely on surveillance by election officials or witnesses.

**Conclusion**

Conducting elections always involves a tradeoff. While Finland’s mode of conducting elections is secure, secret, and straightforward, one could argue this comes at the cost of convenience, especially in comparison to i-Voting in Estonia, mail-in ballots in the U.S., and other forms of remote voting. Why Finland is so dedicated to preserving the secret ballot through surveillance is still up for question. Maybe the dedication to the secrecy of the ballot indicates a highly private society or maybe voter coercion was so rampant that surveillance was the only solution. This paradox of using surveillance to protect privacy is unique to the secret ballot and Finland. According to the MOJ’s website, the presence of election officials is “to guarantee that the elections are trustworthy, the voters may freely express their will, and that secrecy is maintained” (Vaalit Val). In Finland, mandatory secrecy goes beyond constitutional law; “its fundamentals are based on the idea of auto-paternalism and it is understood as a mechanism of self-binding of autonomous citizens in order to avoid situations of external pressure or corruption” (Buchstein, 2004, p. 53). It is not voters who have to provide the necessary means to ensure privacy, nor do voters have to make any decisions themselves, it is the state that must provide the conditions required to ensure the secret ballot. The unique characteristic of the Finnish electoral system undoubtedly is its devotion to secrecy.
Spain

Context

Like Finland and Estonia, the democracy of Spain is relatively new, despite having a deeply rooted electoral system. Prior to the dictatorship that would last thirty-three years, the Spanish people made many attempts at democratization, most notably in 1810-1812 with the writing of the first constitution, nicknamed La Pepa. Following the introduction of electoral laws in 1837, universal suffrage was established in 1869. However, democracy in Spain faced many tumultuous decades, marked by monarchical crisis, fascist dictatorships, military coups, and civil war. General Francisco Franco would rule Spain as a military dictator from 1939 until his death in 1975, marking a period of interruption in the exercise of democratic rights. During these four decades, the democratic flame did not burn out nor “wipe the past or the accumulated experience of a century of electoral legislation, from historic memory” (ACE, 2005). The Constitution of 1812 was modern in ideology, favoring decentralization and republicanism, and it would influence later electoral law. Upon the death of Franco, Spain embarked on a transition from fascism and authoritarianism to democracy. The Constitution of 1812 became the “embryo of electoral law” and a symbol of political freedom for the Spanish people (ACE, 2005). Like many modern democracies, the constitution was a transnational effort that incorporated many ideas from the French revolution and the Constitution of the United States, but it also found inspiration in the old democratic traditions of the Spanish autonomous regions (ACE, 2005).

Legal Framework

To begin the transition from fascism to democracy, King Juan Carlos established the Royal Decree Law on Electoral Norms in 1977 to elect the parliamentary chambers that would
write the new constitution, marking the first democratic elections held in Spain (ACE, 2005). By 1978, Spain had a working constitution that decentralized power away from Madrid and into the hands of 17 autonomous regions, functioning similar to the electoral system in the United States (ACE, 2005). As a unitary state with a parliamentary monarchy government, Spain is organized territorially through three levels of power: state, autonomous communities and local entities. Therefore, the state, autonomous communities, and local regions each have their own elections, but unlike the United States, the centralized election law creates uniformity on election day. The Organic Law on the General Electoral Regime (LOREG) is exceptionally detailed, setting up “an independent complex and hierarchically-framed administrative machinery, aimed at ensuring transparency and objectivity in electoral procedures and observance of the principle of equality” (JEC, 2014). Outlined in the electoral law are the main provisions regarding the electoral system, including issues regarding voting abroad and state responsibility for facilitating voting and the necessity for electoral legislation to be approved by organic law with a special majority (López-Pintor, 2005, p. 83). Overall, the electoral law has the same status as constitutional law (ACE, 2005) making any electoral reform extremely difficult, as the proposed amendment would have to be scrutinized at the highest level.

**Electoral Management**

The transition from fascism to democracy removed the lid on a boiling pot of regionalism and nationalism, as no longer were certain groups like the Basques, Catalans, and Aragonese forced to suppress their individuality. To ensure the transition into democracy went smoothly, the Spanish government was careful to give these groups political power and “took account for the existence of different demands for autonomy vis-a-vis central power” (ACE, 2009).
However, even though throughout the decentralization process regional differences were considered, the Spanish government needed a centralized electoral law to ensure the transition into a consolidated democracy. In contrast to Spain, regional differences abound in the United States, but instead of allowing those regions to decide how elections would be run, Spain chose to assimilate nationalists claims “into the political system through electoral mechanisms underpinning the decentralization process” (ACE, 2005). In sum, the transition from a super-centralized dictatorship to a strongly decentralized state required a balancing act between strong electoral law and decentralized power.

The Spanish government’s sensitivity to regional claims is embedded in the electoral law of 1985 by decentralizing election administration in the 17 autonomous regions. The specifications in Spain's electoral law’s specifications for election administration illustrates how contemporary Spain can be considered as a quasi-federal state (López-Pintor, 2005). There are three levels of elections: national, elections in the autonomous regions and local elections. At each level, the law provides that elections will be conducted under the full supervision of the electoral boards, of which there are three. On a national level, the Central Election Board (Junta Electoral Central, JEC) is an independent and permanent election management board (EMB) that operates regularly. The JEC is a policy-making organ, whose decisions are binding for all the lower regional and local election boards. The JEC is comprised of 13 members, eight of which are members of the Supreme Court and the remaining five come from a variety of academic backgrounds, such as, professors of law, political science or sociology. The lower level election boards follow a similar structure, but with fewer members and lower levels of qualifications.
Spanish electoral boards are not government commissions; instead, they are independent, autonomous, and neutral entities whose objective is to ensure equal and fair elections. Under the JEC’s wing is the Ministry of the Interior, local governments, the Electoral Census Office, and the local polling station committees. The regional and local level boards perform the same functions within their own arenas. Overall, this hierarchical system of electoral administration distributes the responsibility of running elections in a centralized, yet decentralized manner.

Spain’s “mixed model” of electoral management has been in practice since the system was passed into law in 1985 (ACE, 2009). What makes this mixed model work is its “quasi-judicial composition of electoral boards complemented by a state administration which is accepted as effective and impartial” (ACE, 2009). This system of electoral management works for Spain, as the members of the electoral boards have been regarded as professional since their inception and today are seen as essential ingredients to the Spanish recipe of elections (ACE, 2009). Unlike in the United States, their independence from political parties has gained them institutional respect, and so far, Spain has had little contention during elections, which may be the result of their mixed-model of electoral management, clear electoral law, or lack of partisan administers of elections (ACE, 2009).

Secrecy

Although Spain’s election law clearly states in Article 86.1 that the vote shall be secret, election observers report that “this provision is clearly not a matter of concern in terms of the management of the voting system” (OSCE, 2004, p. 7). While Spain’s election law is sturdy, well organized and efficient for managing the election administration, the actual practice of voting does not maintain ballots are kept secret. In this sense, Spanish elections are rather
unceremonious. Voters are allowed to bring in their own ballots printed by political parties, a practice similar to the paper ballot system in place in the U.S. before the implementation of the secret ballot. While the Ministry of the Interior is responsible for printing ballots for the polling stations, having the option to bring ballots into the polling station opens the door for vote buying, voter coercion and intimidation.

Election observers from the OSCE/ODIHR also noticed that voters chose not to use the privacy booths and opted to cast their ballots in full view of everyone present (OSCE, 2004; OSCE, 2015).9 Unlike Finnish voters who have no option but to mark their ballot in the voting booth, Spanish voters can either fill their ballot out before heading to the polls, mark their ballot at the polling station in the privacy of the voting booth, or out in the open. Election observers from the OSCE (2004) describe the scene at the polling station:

The placement of ballots and envelopes on tables in the open at polling stations encourages open voting. Moreover the placement of the booths and tables was such that the voters’ choice could often be easily discerned by observers. In practice, the voting system does compromise the secrecy of the ballot and violates the election law. Current practice may also open the door for possible intimidation, especially in Basque country, where some electors may fear to pick up certain ballots from the ballot table or to vote in a voting booth. (p. 7).

Spanish voters and election officials seem do not seem to value the sanctity of the voting booth as encouraged by their constitution, LOREG, and other international treaties. The Central Election Board’s website says that voters can pass through the voter booth “si así lo deseasen” or “if they so wish.” This hands-off approach is similar to the Estonian government’s approach to voter privacy in that the State should not interfere with its citizens decision making.

OSCE/ODIHR election observers also reported that ballots and ballot envelopes for mail-in ballots were loosely kept (OSCE, 2004). Up until the moment they are placed in the ballot box,

---

9 See Figure 9. Spanish Polling Place.
“ballots are not controlled, but circulate freely” (OSCE, 2004, p. 7). Overall, the voting process is somewhat unregulated and the secrecy of the ballot was not maintained.

Although the importance of the secrecy of the ballot is blatantly ignored during the voting process, one Spanish procedure reinstates voter privacy by erasing all traces of a voter’s choice. After the results of the election are announced, the ballots are destroyed by law, except for those challenged or invalid, according to the OSCE reports (OSCE, 2004; OSCE, 2011; OSCE, 2015c). Article 97 states that ballot papers must be destroyed in full view of those present, except those ballots that have been rejected or challenged ballot papers. On the one hand, this practice of destroying the evidence makes conducting a recount almost impossible, but on the other hand, with no record of the paper ballots, all traces of individual ballots and the possible links to the voter’s identity are destroyed.

In comparison, each state in the U.S. maintains and sells voter records, and even though one’s candidate choice is not available, these records carry personally identifiable information. The Council of Europe’s Code of Good Practice in Electoral Matters states that publishing whether voters voted or not can violate the principle of voter secrecy since abstention may indicate a political choice (Venice Commission, 2018, p. 10). Moreover, political parties and campaigns can use that information about who voted to target future voters. By destroying ballots immediately, Spain eliminates that possibility. Also, this practice prevents voter records from being digitized and the possibility of combining voter records with other data, which may avoid political coercion and intimidation in the future. After the 2016 U.S. Presidential Election and the revelations about Cambridge Analytica, we know that our online habits using social media and our social networks can be very revealing of our political inclinations. Adding voting
records into the mix adds just another data point that can be used to nudge us towards voting a certain way, thereby taking away our right to engage in free and fair elections. While this tradition in Spain was written into law before one could ever predict the proliferation of social media, destroying ballots may be a practice that comes in handy in the future, especially in securing democratic elections.

**Voting Technology**

According to Spanish electoral law, voting must be done using paper; therefore, introducing electronic voting would require amending LOREG. While various forms of electronic voting have been conducted on a pilot scale, the lack of certainty regarding the security of the system prevents wide-scale implementation (Torregrosa, 2018). The electronic voting technologies also proved to be inefficient, as they only speed up the counting process by a few hours. Coupled with the security risks, the JEC halted experimentation, but ironically, the Spanish government would use the weakness of voting technologies to suppress separatists’ movements. Cataluña has long sought the right to self-determination, even though the Spanish government rules any referendum as unconstitutional. In 2017, Catalonians attempted to conduct a referendum through traditional paper-based ballots, but ballot boxes were seized by the Guarda Civil, and mobile voting websites and pages with information on where to vote were shut down. In reaction, Cataluña has plans to introduce an external e-voting system by 2020, in addition to extending electronic voting to all voters (Yakubowski, 2018). So, while electronic voting may be underway in Cataluña, any use of voting technology in future elections will not be recognized as legitimate by the Spanish government until LOREG is amended.
Conclusion

From the outset of the Spanish electoral system, the government was sensitive to the demands of the autonomous communities, which reflected the principle that in a democracy, voters should have the right to decide how they elect those to power. For Spain, this meant coming up with a system that worked within their somewhat irregular political culture. The electoral law, therefore, leaves voters with many options of how to vote, but unlike voting in the United States, the experience of voting in Spain (generally) looks the same from polling place to polling place. While voting technology has been piloted, implementation would mean amending LOREG, a law that has worked to secure democratic elections throughout Spain’s transition into a consolidated democracy. Arguably one of LOREG’s greatest strengths is its balance between the need for decentralizing power to the autonomous regions and the need to create a national standard and protocol for conducting elections. Although abidance by the requirement of secrecy is minimal, the political culture in Spain has formed its own unique traditions on election day. The ballot box, envelopes, and paper ballot system symbolize the Spanish democratic way.

The United Kingdom

Context

The influence of The United Kingdom’s democratic traditions on much of the modern Western world cannot be understated. The United Kingdom was one of the first countries to require the secret ballot legally under the Ballot Act of 1872. Later, the secret ballot would become enshrined in other legal documents, such as Article 21 (3) of the Universal Declaration

---

10 Separatists movement’s adoption of voting technology may hinder the possibility of implementing electronic voting machines.
of Human Rights, Article 25 of the International Covenant on Civil and Political Rights, and Article 3 of the European Convention on Human Rights. Even though democracy is a relatively new chapter in England’s history book, elections have deep roots in the English political culture. Before the secret ballot, voting in England was conducted via a show of hands at the ' hustings' (a temporary, public platform from which candidates for Parliament were nominated), a practice brought over to Colonial America. Because a landlord or employer could see how their employee or tenant voted, voters could be intimidated to vote a certain way to save their job. Freedom from coercion or intimidation at the polls was just one of the political rights that would be advocated for by a powerful movement called the Chartists. In their 1838 petition, the Chartists demanded that “the suffrage, to be exempt from the corruption of the wealthy and the violence of the powerful, must be secret” (The People’s Charter, 1838). Despite their campaigning for secrecy in elections, British Parliament would not act until the Ballot Act of 1872 which initiated the confidentiality of the ballot. Since then, suffrage has expanded, but the actual practice of conducting secret ballot elections has remained relatively the same.

The United Kingdom’s elections have recently entered the global spotlight as the political culture seems divided on the decision to leave the European Union. At the time of writing this paper, the United Kingdom remains a member state of the European Union for the time of being. If and when the U.K. leaves the E.U., the electoral system will most likely not change, considering how little the U.K.’s voting system has changed since 1872. Therefore, for the purposes of this paper, the United Kingdom should not be defined by its membership, as its differences to other member states remain even if Brexit is fulfilled.
Legal Framework

One of the key differences between the United Kingdom and other Western democracies is that the U.K. does not have a single constitutional document as do Estonia, Finland, Spain, and the United States. Unlike the omnibus electoral laws in Spain, Estonia, and Finland, the United Kingdom has many electoral laws, some of which date back to 1695. With over 50 primary and over 170 secondary pieces of legislation, the UK’s legal framework is “voluminous, fragmented, and repetitive” according to the OSCE (2015d) report (p. 1). There are many overlapping pieces of the primary legislation visible in the names of the various acts: the 2000 Political Parties, Elections and Referendum Act, the 2006 Electoral Administration Act, and the 2009 Political Parties and Elections Act. Secondary legislation includes statutory instruments, rules, and codes of practice (OSCE, 2015d). Every electoral reform adds on to previous voting protocols, without abandoning the law altogether. As a result, the OSCE (2010) recommended that the “legal framework for the elections should be consolidated, simplified and modernized through the conduct of a comprehensive review of all relevant legislation and legal acts” to improve the transparency and accessibility of electoral laws (p. 5).

The UK’s Electoral Commission (EC) set out to review their electoral law, recognizing the difficulty in administering elections while abiding by over 200 acts, regulations, and orders. The EC asked law professor, Dr. Bob Watt, to evaluate the UK’s electoral laws. In Watt’s (2013) report, he argues that the UK’s electoral law can be simplified, modernized, and reorganized by changing the structure, not the content, of the UK’s electoral law. As of 2019, consolidation of the electoral law is still pending, which may be to Parliament’s preoccupation with leaving the
European Union. Yet, acknowledging the weaknesses in their complex electoral system is a significant step.

**Electoral Commission**

The body responsible for issuing the report, the Electoral Commission (EC), was established in 2000 under the Representation of the People Act to assist with electoral management. Since then, the EC has expanded their role from aiding and issuing recommendations to local election offices to becoming the source of expertise on electoral law and now yields significant power over local authorities (James, 2009). As an independent body from the government, there is a push and pull between the EC, Parliament, and precedent which Watt (2013) describes:

Electoral law has a number of subjects, and a number of problems have been identified below in respect of their respective positions. It is acknowledged that the Electoral Commission has produced helpful guidance which goes some way towards ameliorating the problems. However, no commentary or guidance can replace legislation which remains the primary source of obligations. Furthermore, the existence of even the most helpful guidance does not mean that the law itself should remain confusing (p. 16).

Concurring with Watt’s assessment, James (2009) argues the EC continuously wants more power over local authorities, which would make the UK’s electoral system more centralized than its current decentralized nature of electoral administration. However, because of the uncodified nature of the British constitution, the EC - like any public organization - could be abolished by a majority in Parliament at any time (James, 2009). Similar to the United States, the administration and organization of elections in the U.K. is up to local government authorities; however, local authorities are bound by national electoral laws in the United Kingdom (OSCE, 2010). Still, the EC’s influence is much more significant in comparison to the American equivalent, the Election Assistance Commission. In the U.K., the EC is exceptionally influential in pushing the electoral reforms that local election administrations must follow; therefore, even though the EC cannot
punish local election administrations for noncompliance with their recommendations, their legal influence is a vast source of power.

Secrecy

In the United Kingdom, the process of conducting an election with secret ballots has changed little since the Ballot Act of 1872, but one could argue that their system never met the requirements of a secret ballot at all. In national elections, the United Kingdom implements a vote tracing system to prevent voter fraud and impersonation. Every ballot paper bears a serial number or QR code that is linked to a voter’s unique registration number.11 At the polling station, the voter must check in and provide the poll worker with their name and address, with which the poll worker will search in the electoral register. The electoral register contains the names, addresses, and unique identifying number of everyone who is registered to vote. The ballot numbers appear in two places: one on the ballot itself and the other in a record book, where the poll worker will write the voter’s unique identifying number next to before handing them their ballot. The voter then heads to the polling booth to cast their vote in private. Voters place their completed paper in a ballot box, which is locked and sealed at the start of polling and is not opened until it arrives at the counting center. At the close of the polls, the ballot papers and the corresponding number list are then sent to the counting office. After election day, the ballots are sealed in packets and can only be accessed with legal authorization from the election court as part of an investigation into allegations of electoral fraud (Maley, 2000).

Vote tracing allows for cases of electoral or voter fraud to be investigated systematically. However, since one’s identity is associated with their ballot, is the secrecy requirement violated?

11 See Figure 10. Example of a Ballot Paper in the United Kingdom.
The Electoral Commission holds that there are strict protocols in place to prevent voter privacy violations and that the vote tracing system is imperative to address allegations of fraud (Electoral Commission, 2006). Ballot papers can only be accessed by order of the High Court or Parliament itself; however, rumors of abusing the system to identify voters do exist. One report in The Guardian claims that in the 1960s, the vote tracing system was used to identify those who voted for communist candidates and that information was sent to M15 (Wilson, 2011). While unsubstantiated, one can see how the vote tracing system opens the door to potential misuse.

In comparison, if one were to obtain a voter registration list and ballot boxes in the United States, it would be impossible to figure out how someone voted because American ballot papers do not bear any personally identifiable information. The vote tracing system raises suspicion and uncertainty about what happens to the ballots after they are cast. The Electoral Commission’s Ballot Secrecy Factsheet (2006) admits that while it is theoretically possible to identify who cast a particular vote, it can only be done under the orders of the election court. For one year, the ballot papers are sealed and kept in storage in case of potential corruption or fraud allegations. After one year and one day, the ballot papers are incinerated and destroyed so that there are no permanent records of votes, similar to Spain (Game, 2015).

Vote tracing yields a unique counting protocol, which occurs in a two-step process. First, ballots are counted using the corresponding ballot identification numbers to ensure the correct number of ballots have been cast per number of voters who attended election day. Then, the Presiding Officer transports the ballot boxes to the counting center, where they are essentially dumped on a table (in full view of the anyone who decides to watch) and counted by hand.  

---

12 See Figure 11. Counting Process in the United Kingdom.
During this dumping process, ballot papers are mixed to preserve the secrecy of the vote, according to the EC. Next, count teams sort the ballots by the candidate and once completed, the results are announced, the ballots are sealed, and the boxes are sent to a secure storage place. The UK’s meticulous counting process results from their vote tracing mechanism, which is seen as a solution to potential allegations of impersonation.

So, why does the United Kingdom use a system that violates the secret ballot requirement that is clearly laid out in their own laws and international covenants? Since 1872, the British traced their votes in the event of a challenge or to prove one has been impersonated, and since then, the system appears to work. In 2017, one case of voter impersonation was reported at the polling station, and the perpetrator was convicted. The secret ballot alone cannot thwart undue influence, corruption, and vote buying practices. Instead, the election officials, voters, and election procedures need to work in coordination. For U.K. citizens, having the ability to challenge ballots is a normal part of their voting system. Still, the Electoral Commission reassures voters that from the moment ballots are printed to the moment they are incinerated, the papers are under the watchful eyes of election officials.

Estonia, Finland, Spain, the United States, and the majority of democratic nations avoid voter fraud and impersonation by requiring voter identification. In the United Kingdom, voters over the age of 18 can go to the polls and simply provide their name and address to the poll workers to receive their ballot. Requiring voter identification certainly is not a perfect system. In the United States, the debate over voter ID laws morphed into a partisan battle over citizenship. However, the Election Commission acknowledges that requiring voter could be beneficial to their voting system and in 2014, they recommended voters should be required to provide proof of
identification. By 2016, the U.K. Government asked local councils to conduct pilot tests in 2018 to test different ways of identifying voters at polling stations. Pilot testing allowed local administrations to see what impact the electoral reform would have on the voting process before implementing it in a national election. Pilot testing in the United Kingdom is exceptionally methodological, evaluating election reforms from all perspectives of the voting system - voters, election officials, and candidates.

**Electronic Voting**

When considering implementing new technologies in the United Kingdom, the Electoral Commission traditionally tests the reform in many small-scale pilots in local elections. Once a new voting mechanism has been tested, a multipart evaluation and careful analysis are conducted long before implementing the new voting system. The multipart assessment helps to determine the technology’s effect on factors such as turnout, fraud, and the electoral administration (Alvarez & Hall, 2008). Public attitudes toward new technology are taken into consideration as well. These detailed reports are produced with evaluative data made available for other researchers, policymakers, and the public to additionally analyze (Alvarez & Hall, 2008). The United Kingdom has had far fewer scandals than their neighbors across the Atlantic, most likely because they test voting technologies in concentrated areas, on small scales. Since most electronic or mechanical voting methods introduce as many problems as they solve, the United Kingdom has stuck to hand-counted paper ballots. The United Kingdom has had fewer election-related scandals than the United States, most likely because of their rigorous piloting process for testing changes to their electoral system. In the United States, pilots are conducted on the local
and state level, often without the same resources that are afforded to local election authorities in the United Kingdom under their centralized election administration.

Hand-counting paper ballots in the United States is inconceivable considering the frequency of elections, population size, and the human resources it would require. In the United Kingdom, the biggest push for testing electronic voting was to increase the speed of results, something which Americans are rather accustomed to. Also, voting technologies were tested to see if the accuracy of the counting procedure improved. Between 2000 and 2007, 156 pilots were conducted on postal voting and electronic voting in a variety of locations. In 2007, six election councils tested electronic counting, and the results were of mixed outcome. Some districts found few technical difficulties; others proved to be so problematic that e-counting had to be abandoned and officials reverted to a manual count mid-election. In these cases, a standard manual (human) count would have been faster than using electronic means.

Using technology raises additional concerns, such as, voter familiarity with the technology used, questions of the digital divide, heightened security risks as with foreign interference, risk management plans, which would require structural changes from decentralized election offices to a central computer. Five different pilots of e-voting were conducted in 2007, testing remote internet voting, telephone voting, and the use of supervised, networked electronic facilities at polling stations. Overall, since cyberattacks cannot be entirely prevented, electronic voting technologies have been put on the back burner. To learn about e-voting, the United Kingdom studies other countries’ experiences with the techniques as well. However, putting the technologies to the test within their own political context was vital.
Testing new voting methods is not unique to the United Kingdom. Finland, Germany, France, and Norway each trialed electronic voting mechanisms; however, pilot testing in the United Kingdom seems to be as regular a practice as voting itself. The United States, in contrast, is rather quick to throw new election technology into the mix, without detailed evaluation and consideration of such academic studies. Also, too often changes in the American electoral system are poorly communicated to voters (Alvarez & Hall, 2008). Alvarez and Hall (2008) show how unique the UK’s pilot testing is in comparison to the way the United States implements new technologies:

The American model of electoral reform implementation can be contrasted with the more deliberate model of implementation that has been found in Europe, where election reforms are more often pilot-tested under controlled conditions before being implemented in a large scale. This has been especially true in the area of electronic voting technologies and convenience voting in the United Kingdom [...]. The United Kingdom provides a model of how such pilot testing can be done, in contrast to the way in which such tests occur in the United States (p. 72).

In the United States, pilot tests are often large scale, nonscientific tests. In contrast, the Electoral Commission conducts regular surveys, public opinion polls, focus groups, and policy analyses when evaluating voting systems (Alvarez & Hall, 2008). This bottom-up feedback allows for previously unnoticed problems to emerge and areas for improvement to become apparent. In sum, the UK’s approach to electoral reform seeks to find socio-technical solutions that fit their political culture and context, not just technical ones.

**Conclusion**

The United Kingdom’s hand-counted paper ballots and vote tracing system represent the importance of tradition in their electoral process. However, from the rigorous pilot testing reports, we can assume that the United Kingdom is not opposed to change or modernization, but that change must be warranted. Technology introduces new problems, problems that are continually changing and evolving just like the societies who use them. As elections grow
increasingly reliant on technology - with online voter registration, delivery of election results, and electronic voting machines - the United Kingdom chooses to weigh the benefits against the costs. Rather than relying on anticipation of risks, the UK systematically tests new technologies in real-world situations. The Electoral Commission’s evaluations and reports are readily available online for voters, election officials, and the international community to examine. Overall, the UK’s pilot testing reflects the first principle of democracy: that the power given to the citizens fixes the political direction of the country and that the elected delegates come afterward to implement their decision (Owen & Lardeyret, 2010).

The United States

Political System

To the rest of the world, American elections (and Americans) are different and crazy and complicated for many reasons. Campaigns begin as fast as they end. Candidates raise hundreds of millions of dollars to spend hundreds of millions of dollars. They hire armies of coaches that prepare them for televised battles, campaign rallies, and conventions. Voters put bumper stickers on their cars, signs in their yards, and wear stickers on their shirts. They discuss who they think will be the next president at the dinner table, on social media, and at work, until - finally - election day arrives. Americans head to their polling station and cast their ballot, but how they cast their ballot depends on where they are from. Some bubble in their candidate of choice, others touch their name on the screen, punch a hole in a piece of paper, or lick an envelope. One’s grandmother, brother, father, and sister, can all vote using different methods to cast their ballot. No matter how they vote, their ballot will only represent who they hope will be president-
elect, because, in the end, only 538 people technically get to vote the president into office, thanks to the American Constitution.

**Context**

Voting has always been a bit more chaotic on this side of the Atlantic. Early elections in the United States were highly public events conducted without secrecy or privacy. Typically, voters went to the town hall, stood in front of a judge with their hand on a bible, and voted out loud for everyone to hear with no secrecy and even no ballot. Without a form of a physical ballot, keeping track of votes was done by one person, but anyone nearby who wanted to make their own record could if they so desired. On the one hand, public or open voting ensures complete trust and transparency of elections, but on the other hand, voting out loud made any contested results impossible to verify. One would have to trust the tabulators notes and their counting abilities. Another downfall of the open voting system is that since one could hear how their fellow citizen voted, politicians, landowners, and wealthy could (and would) try and influence or intimidate the voter using techniques, such as, blackmailing, vote buying, “cooping” (kidnapping someone to prevent them from voting), and consuming copious amounts of alcohol. As one can imagine, election days were fraught with violence and corruption. However, many saw the voting as a public duty that protects deliberative democracy by requiring one to defend their choice and those who chose not to vote had something to hide (Engelen & Nys, 2013).

In an effort to cope with the growing violence, rising population, and expanding suffrage, local governments began conducting elections at polling stations using paper ballots elections, but not yet with the secret ballot system. Voters would have to bring their own ballots, which were colored differently according to a political party, and only allowed for voters to choose
from that party’s candidates. Ballot boxes and colored paper ballots ushered in a new wave of problems. For example, some bad election officers designed ballot boxes specifically for stuffing votes. Problems with oral ballots persisted with the paper ballot system since voters could still be bought, blackmailed, and suppressed as the system still lacked anonymity. One could quickly identify how the voter was voting because they carried in a colored ballot. As other countries began adopting the Australian ballot and the United States followed suit; however, on a state by state, city by city basis. Every electoral reform would occur this way as this is what the Election Clause of the Constitution permitted. While a small number of changes of great importance to the Constitution, the importance of secrecy in elections has never been constitutionally determined.

**Legal Framework of the United States**

The right to vote is at the core of the American political system, yet the United States Constitution says very little about how elections will take place and who can exercise that right. When the Constitution was being written, Americans had just gained their independence from the most centralized form of government: a monarchy. In order to safeguard the new nation from a centralized tyrannical rule, the conduct of elections would be self-determined by each state. Article 1, Section 4, Clause 1 of the United States Constitution reads: “The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators.” This clause left out two important specifications: who has the right to vote and how those citizens will vote. Who has the right to vote would continue to be modified at a federal level. The right to vote gradually expanded to be
exercisable by all United States citizens, regardless of race (14th and 15th Amendment), gender (19th Amendment), and age (24th Amendment). These reforms are of monumental importance; however, how citizens vote is the focus of this paper.

The Secret Ballot in the Law

As the United States grew in size and population, the complexities of electoral law would grow as well. Today, each of the 50 states has their own constitutional provisions or statutory requirements for the secret ballot. Forty-four states have the secret ballot in their constitution while the remaining 6 have statutory provisions (Fitzgerald, Smith & Goodman, 2017). Fourteen states do not specifically use the word “secret” ballot or “secrecy” of elections in their constitutions, but these states do have either state laws or case law that mandate secret ballots (Keller, Mertz, Hall & Urken, 2006). In six states violations of ballot secrecy are criminalized and in Nevada, revealing your vote is considered a felony. In Delaware, if an election officer violates a voter’s secret ballot, they could be imprisoned for two to five years and in Maine, an election official could serve six months, regardless if they were acting intentionally or not (Del. Code Ann. tit. 15 § 5122. as cited in Fitzgerald, Smith & Goodman, 2017). Although voter privacy is not federally determined, the United States as a whole is devoted to the secret ballot. However, the irregularity of the legal language and punishments associated with violating voter privacy specifically indicates varying levels of importance of secrecy and generally shows how inconsistent electoral laws can be across state lines.

As nations in the European Union, the United States is a party to international laws and standards that stipulate that elections should be held by secret ballot. Article 21 (3) of the

---

13 Delaware, Maine, Michigan, Nevada, and New Jersey (Fitzgerald, Smith & Goodman, 2017).
Universal Declaration of Human Rights and Article 25 of the International Covenant on Civil and Political Rights both state that elections should be held by “secret ballot,” but unlike other signatories, the United States has not incorporated these standards into federal law (OSCE, 2016). Election reform typically comes from the court's jurisprudence. In 1992, the Supreme Court held that a Tennessee statute forbidding candidates from campaigning within 100 feet of a polling place entrance did not violate the First Amendment. The Court stated that:

In sum, an examination of the history of election regulation in this country reveals a persistent battle against two evils: voter intimidation and election fraud. After an unsuccessful experiment with an unofficial ballot system, all 50 States, together with numerous other Western democracies, settled on the same solution: a secret ballot secured in part by a restricted zone around the voting compartments. We find that this widespread and time-tested consensus demonstrates that some restricted zone is necessary in order to serve the States’ compelling interests in preventing voter intimidation and election fraud (Burson v. Freeman, 1992, 504 U.S. 191).

This decision insinuates that protecting voter privacy can be a method of preventing voter fraud and thwarting against undue coercion. The Court went one step further in signaling the importance of the secret ballot. In the 1995 case McIntyre v. Ohio Elections Commission Code, the Court upheld that the right to distribute anonymous campaign literature is protected by the First and Fourteenth Amendments. The Court wrote:

The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible [...] the Court's reasoning [in an earlier case] embraced a respected tradition of anonymity in the advocacy of political causes. This tradition is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation (McIntyre v. Ohio Elections Commission Code, 1995, 514 U.S. 334, 341-43).

The Supreme Court’s jurisprudence highlights the importance of anonymity in preventing voter intimidation and electoral fraud and the social value in protecting one’s privacy through the secret ballot. Although the Supreme Court helps solidify the value of the secret ballot, the effects of the ambiguous Election Clause would eventually lead to electoral crisis, forcing the Court to effectively decide the outcome of the 2000 U.S. Presidential Election Court.
The 2000 United States Presidential Election

The problems with the United States voting system accumulated into the perfect storm that was the 2000 Presidential Election. Typically, election night ends with one candidate calling the other to concede, but the night of November 7th, 2000 was just the beginning. Between 7:50 and 8:00 pm, all major news networks declared candidate Al Gore the winner based on exit polls. Just two hours later, the networks retracted their predictions and returned Florida to the ‘undecided’ column, where it would remain for the next month. The following morning, Gore called Bush to concede after the networks prematurely announced Bush was in the winner. Then, reports of voting machine miscount and ballot design failures came pouring in from Florida, igniting Gore to retract his concession and file for a recount. The nation began sifting through Florida’s electoral law finding many contradictions, loopholes, and vague language. According to Florida electoral code, if the winner won by less than 0.5% of the votes, they could call for a statewide machine recount (Fla. Stat. §102.141(7)). After revelations about old voting machines failing and poorly designed ballots, the Gore team - under the state’s election code - was allowed to protest the results in up to three precincts and request a manual recount. However, it was up to the individual county canvassing boards to decide whether to do the recount and how they wanted to do it. Lawsuits were filed by both Bush and Gore, as the partisan accusations flourished into a national legal battle. Without clear electoral law, without uniform sets of standards for local administrations must follow, and without a president-elect, the Supreme Court stepped in as a referee.

As election expert Roy Saltman (2006) writes, “the court would characterize the different standards by which votes are determined in different counties as a violation of that simply
worded but consummately sublime clause of the 14th Amendment clause” which says that no state shall be able to deny any person equal protection of the laws (p. 2). In a 5-4 decision, the Supreme Court halted the statewide recount because they ruled it violated the Equal Protection Clause. The Court’s decision ended the partisan seesaw ride Americans had been on for the past month, and George W. Bush became the 43rd President. After the election, many began to realize that the administrative, legal and technological systems of the American electoral process were horribly flawed. Overnight, the legitimacy of a trusted set of institutions, officials, and the democratic process was called into question.

If the problems of 2000 were not addressed before the next presidential election, the government risked further damaging the legitimacy of the American electoral system. Following the election, former Presidents Jimmy Carter and Gerald Ford chaired a bipartisan commission that issued a report on how to improve the electoral system. Congress incorporated some of their suggestions into the Help America Vote Act of 2002 (Pub.L. 107–252). The goals of HAVA, as it is commonly known, were to replace punchcard and lever-based voting machines, to create the Election Assistance Commission who would assist in the administration of elections by establishing minimum standards and guidelines. In order to restore trust in the American elections to prevent further depressing the participation and faith in the democratic process, federal action was deemed necessary.

Though despite HAVA’s efforts, it failed to address the real problems with American elections: the decentralized structure of election administration, the lack of uniform standards, and the poorly designed voting technology. Lawmakers wrongfully accused paper as the enemy and assigned technology as the solution (Simons as cited in Leovy, 2017). The failure was not
paper ballots, but the technology that used the paper and the election administration behind the
design of the ballot. For that reason, replacing the voting machines did not end Florida’s
continued election day troubles, but instead, it temporarily masked the problem. In sum, HAVA
deflected the attention away from the administrational problems by offering technical solutions.

**Electoral Administration**

The irregularities between the state’s electoral laws are representative of the disorganized
structure of election administrations and authorities. With over 10,000 counties, 113,754 polling
places, 245.5 million citizens over the age of 18, and with 50 different electoral systems, there
are literally thousands of ways elections are conducted in the United States (U.S. Census Bureau,
2017). The decentralized model allows for relatively independent election authorities to run
elections within their state and local laws. Many argue that the localized structure is a strength,
as it allows for diversity, tradition, and state/local autonomy. Idealistically, putting the power in
the hands of the many safeguards against those at the top manipulating the system and
controlling the outcome of elections. In reality, the decentralized electoral administration
maximizes opportunities for partisan interests and generates a lack of uniform standards (Norris,
2016). The lack of a strong, professional election administration hinders the ability to establish
uniform standards for voting.

When local election administrations have support from and oversight from a centralized
organization, such as, in Estonia, Finland, Spain, and the United Kingdom, these countries are
able to establish uniform opening times for polling places, training for election officials and poll
workers, receive funding for voting equipment, and assistance in designing the ballots. The voter
experience is also enhanced, as voters can refer to a government website for a one-stop shop for
all information on how to vote. The United Kingdom's government-centralized model allows the election authorities access to resources from the public sector. Centralized election authorities benefit from having a clear chain of command and accountability, which comes in handy when problems arise (and they always will arise). Overall, it lessens the heavy burden of conducting an election by offering channels of support. HAVA is the only national law that has tried to tackle the issue of election administration, but it was relatively ineffective in doing so. States were given the option to adopt standards in order to receive funding from the Election Assistance Commission (EAC). Established by Title II of HAVA (Public Law No. 107-252), the EAC is “an independent, bipartisan commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration” according to their website. One of the EAC’s roles is to accredit the testing laboratories and certify voting systems. Like the United Kingdom’s Electoral Commission, the EAC does not have the authority to enforce uniform standards, but the Electoral Commission has been far more influential in standardizing elections.

The partisan nature of United States elections and the decentralization of authority encumbers the ability to establish our own centralized election management body. However, Pippa Norris (2016) argues in favor of creating independent agencies made up of experts from various fields (as the UK and Spain did) because it insulates election officials from outside pressures and “helps to curb any potential conflict of interest, partisan meddling, and the abuse of power by external forces, especially where it is suspected that the electoral arbitrator is biased towards incumbent politicians, political parties, the governing party, or powerful elites” (p. 20).
If an independent agency is responsible for creating standards, rather than elected officials, there is only one set of rules for politicians to abide by.

Without an independent election administration, the state and local authorities continued to suffer from partisan battles in 2018 just as they did in 2000. In many states, the authority over elections is the secretary of state, and as an elected official, it is no coincidence that the party affiliations of the secretaries tend to correlate with the outcome of elections. In Florida during the 2000 election, Secretary of State Katherine Harris not only co-chaired George W. Bush’s Florida campaign but also was accused of interpreting the Florida election laws in such a way that favored the Republican candidate. Partisan accusations could have been mitigated if there were a uniform federal election law or an independent, bipartisan election administration.

In 2018, Georgia was plagued by a similar problem; however, this time in a gubernatorial election. Republican candidate for governor Brian Kemp was also the current Secretary of State, making him in charge of running his own election. Lawsuits were filed against Brian Kemp for engaging in practices that suppressed voters by the Democratic candidate. Culpability aside, it is remarkable that elections are considered to be free and fair when the person in charge is also running for office. This is like letting a poker player blatantly deal the cards he wants to himself and others. Worse, it disenchant voters from participating in the democratic process because they perceive the election to be slanted. Rather than leaving elections up to partisan elected officials, there should be an independent or bipartisan agency who creates standards to prevent this from happening. Ethically speaking, all citizens should have the same basic right to participate and vote regardless of what state they are from.
Voting Technologies

The 2000 high-stakes recount threw an embarrassing spotlight on antiquated voting machines that used paper ballots. There were hanging chads, as well as, dangling, dimpled, pierced, pregnant, and swinging ones - all studied under a microscope to determine voter intent.\(^\text{14}\) In addition to problems associated with the punch card system, there was the infamous butterfly ballot - a poorly designed ballot that led voters to think they were voting for one person when they were voting for another, resulting in over and undervotes.\(^\text{15}\) Misleading ballot design is not uncommon, but in a close election, the design of the ballot can have a major impact. For these reasons, the scapegoat of the 2000 election was the paper ballot. Pamela Smith says after 2000, “People didn’t want that image of the guy with the magnifying glass and the chad [...] People were thinking: What’s the furthest thing away from a punch-card system?” (as cited in Smiley, 2016).

HAVA attempted to solve all of the problems of 2000 - whether they be legal, constitutional, administrative, or partisan - by upgrading the technology. However, both the technology that was being replaced and the new voting technologies were not recommended by cybersecurity experts. In fact, cybersecurity experts warned against it decades before. In 1988, Roy Saltman of the National Institute of Standards and Technology (NIST) issued a report to the United States government on the security of electronic voting systems. In his report titled "Accuracy, Integrity, and Security in Computerized Vote-Tallying," Saltman (1988) not only recommended abolishing punch-card voting systems, but also warned extensively on the

\(^{14}\) See Figure 12. The Five Different Kinds of Chads.
\(^{15}\) See Figure 13. Palm Beach’s 2000 Butterfly Ballot and Figure 14. Votomatic Voting Machine Used in the 2000 Election.
unreliability of DRE, other computerized voting machines, and cautioned against any voting machine that does not produce paper records. Most European countries, especially the United Kingdom, thoroughly test any electoral reform (prior to adoption) to see how the change affects all stakeholders in the system. However, the American way seems to be to ignore the ample amounts of incredible cybersecurity and computer science research and purchase faulty systems.

Many of the machines purchased after HAVA were still in use in the 2018 midterm elections, making them over a decade old. Expert warnings about the hackability of outdated voting machines spread before the 2016 Presidential Election. On the eve of election day, the Department of Homeland Security reported that Illinois and Arizona’s online registration systems were hacked, putting not only voters’ personal information at risk, but also threatening the integrity of the election (OSCE, 2017). The ways in which one can hack optical scan machines and DRE voting machines are well documented by cybersecurity experts (Zetter, 2018). Some of these experts even held a hacking convention called DEFCON, inviting hackers from all over the world to see how fast they could hack the various voting machines used across the country.\textsuperscript{16} Cybersecurity experts and election researchers issued a report after the event. It took hackers only two minutes to tamper the results of a machine that was currently in use in 18 states.\textsuperscript{17} They found that a voting tabulator in 23 states is vulnerable to remote hacking through a network attack and “hacking just one of these machines could enable an attacker to flip the Electoral College and determine the outcome of a presidential election” (Blaze, et al., 2018, p. 5). Also, some machines allowed hackers the ability to wirelessly reprogram the electronic SIM

\textsuperscript{16} Such as, Matt Blaze from the University of Pennsylvania, Jake Braun from the University of Chicago, Harri Hursti founder of Nordic Innovation Labs, David Jefferson of Verified Voting, Margaret MacAlpine of Nordic Innovation Labs, Jeff Moss of DEFCON.

\textsuperscript{17} It takes the average voter six minutes to vote.
card used to activate the DRE voting machine that millions of Americans actually use. Their findings gained considerable media attention, so much so that DEFCON has become one of the quintessential examples of the vulnerability in voting technology.

The government often tries to reassure the public by arguing that the decentralized structure of our election system hinders the potential of widespread hacking on an actual election day. In a 2017 Congressional hearing on election security, Louisiana's Secretary of State, Tom Schedler, argued that just because it is technically possible to hack elections does not mean it is logistically feasible. A bad actor would have to sneak into 64 warehouses across the state of Louisiana, break into 10,200 machines undetected and under video surveillance, unscrew the back panel of the DRE, introduce the software, and leave after making the machine appears untouched. According to Pippa Norris (2016), however, it would only take a few minor security breaches to some voting machines, digital registers, or software aggregating vote tabulations in a few polling locations in three or so swing states to “reduce the credibility of American elections, throw the outcome into chaos, and trigger doubts about the legitimacy of the eventual winner of the presidential contest” (p. 7). In other words, the feasibility of tampering with an election, even in a decentralized system, is much simpler with electronic voting machines. Any computer can be hacked; therefore, “the best defenses are ways to audit the election and count the votes outside of, independent of the hackable computers” (Appel, 2016).

In an article aptly titled, “America Continues to Ignore the Risks of Election Hacking” Sue Halpern (2018) describes the various ways in which the voting machines can be hacked, how

---

18 Joint Hearing Before the Subcommittee on Information Technology and the Subcommittee on Intergovernmental Affairs on the Committee on Oversight and Government Reform
results can be intercepted during transmission, and other failures of electronic elections. The National Association of Secretaries of State wrote in a briefing paper that “our diverse and locally-run election process presents serious obstacles to carrying out large-scale cyber-attacks to disrupt elections, and that standalone, disconnected voting systems present a low risk” (NASS, 2017, p. 2). Still, the intelligence community, computer scientists, and hackers have found that decentralization is a deterrent, not a defense (Halpern, 2018). Pippa Norris (2016) writes that “Among all mature democracies, the nuts and bolts of American contests seem notoriously vulnerable to incompetence and simple human errors arising from the extreme decentralization and partisanship of electoral administration processes” (p. 9).

The Decentralizing Effect

After years of decentralized election administrations with differing needs, preferences, and opinions about voting technologies, the United States has a patchwork quilt of voting technologies. As of 2019, there are five broad classes of voting technology: hand-marked paper ballots, mechanical lever machines, Direct Recorded Electronic (DRE) machines, ballot marking devices (BMD), punch card machines, and optical scanners. Optical scan and punch card voting systems combine hand-marked paper ballots with technology. With a mechanical lever, BMD, and DRE voting machines, the ballot is not marked by a human, but it is either mechanical or digital. Each has to be programmed before every election, updating the ‘software’ with the candidates' names and each capture voter choices internally in purely electronic form. As of 2019, there are few if any punch card or mechanical lever machines in use. Between the DRE,

---

19 See Figure 15. Patchwork of Voting Technologies Across the United States.
20 See Figure 16. Premier/Diebold AccuVote OS Optical Scan Machine.
21 See Figure 17. ES&S’s AutoMARK OS Ballot Marking Device.
BMD, and optical scan voting machines, over 15 private companies are responsible for manufacturing the machinery of democracy. Between these 15 companies, they could have anywhere from 3 to 10 different models or versions of various machines. Election Software & Services, for example, has made the AutoMARK, DS200, DS850, DS450, ES&S ExpressVote, InkaVote, iVotronic, Model 100, Optech IIIP-Eagle, Votomatic, Models 150, 550 and 650 (Verified Voting).

Within any given state, there could be a number of combinations of technology. Take the state of Ohio, for example. There are three different ways of voting in the 88 counties in the state of Ohio. About half of those counties use paper ballots and the remaining half use a combination of optical scan voting machines and DRE voting machines with VVPAT, while the others use a combination of optical scans and BMD voting machines. Five vendors are responsible for all the voting machines in Ohio: Election Systems & Software, Unisyn Voting Solutions, Dominion Voting Systems, Premier/Diebold, and Hart InterCivic. In the 2018 midterm election, there were 18 different machines used in Ohio: AccuVote OS, AccuVote OS CC, AccuVote OSX, AccuVote TSX, AutoMARK, DS200, DS450, DS850, eScan, eSlate, ExpressVote, ImageCast Central, ImageCast Evolution, iVotronic, Model 100, Model 650, OpenElect OVI, and the OpenElect OVO (Verified Voting, 2018).

Within the counties themselves, various models will be used. Take Putnam County for example. Putnam County uses either the AutoMARK ballot marking device or the Model 100 optical scan in the polling station. For absentee voting, Putnam County election officials either use the Model 100 or Model 650 optical scan voting machines. In total, Ohio’s 23,787 registered voters in the 24 precincts will vote on one of 11 different machines, according to Verified
Voting’s Verifier. Election officials used nine different machines to enter absentee ballots. This level of complexity is just one state. Nationwide, there are 55 different models of voting machines in use, and within each of the 50 states, each has chosen their own combination of voting machines. In comparison to Spain, Finland, and the United Kingdom who have just one method or machine that counts votes, the United States has thousands.

The complexity does not stop there. Each state has its own way of appointing who is in charge of elections as well. At the state level, the election authority can either be elected, appointed by a state official, appointed by a board, or the board themselves can be in charge, of which they are either appointed or elected. Who does the appointing varies from the Governor, State Elections Commission, State Board of Elections, State Legislature, or the State Senate. Lastly, at the local level, elections can be run by a single individual, a board, a commission of elections, or a combination of two or more entities. Of the 22 states who have a single individual who administers elections at the local level, that individual may only administer elections in larger counties while a board does the smaller counties, they may be elected, or appointed. That sole individual may appoint another individual to administer elections. In 18 states, the local election administration duties are divided between two or more offices and the remaining ten states use a board of elections for the primary responsibilities of local election administration (NCLS, 2016). It goes without saying that the United States electoral structure is complicated, unorganized, and decentralized.

**Conclusion**

The United States was founded under the idea that its citizens have inherent natural rights, so naturally, the chaotic, decentralized nature of American elections reflects the heart of
American political culture. There has always been a method to our madness. If the federal government had the ability to seize or control state elections, the system would become unbalanced, and election results would most likely not reflect the will of the people. Elections are as much about representation as they are about power, and power needs to be dispersed to prevent authoritarian rule. On the one hand, the separation and decentralization of power have allowed states to experiment with different voting systems without causing national chaos.

Decentralization allows states to conduct elections according to their specific needs whether they be cultural, geographical, or population-related. For example, New York City’s election office faces many different election day challenges than Butte Montana’s election office. The Election Clause allows them each to experiment with policies that work for them locally. At the end of the day, each citizen’s vote has much more influence over their state’s politics than national politics, so by preserving state power, citizens preserve their own.

On the other hand, decentralization has led to disjointed, inconsistent, and detrimental application of electoral laws, procedures, and voting methods. Oftentimes, this diminishes confidence in the democratic process. It is no wonder the United States has one of the lowest turnout rates among the world’s most developed countries. Centralizing elections could increase turnout. In the 21st century, U.S. citizens leave their home state far more frequently, and when one’s ballot is tied to a state they are not currently residing in, one has to take many, many steps to exercise their right to vote. Although we are the United States, citizens should be able to vote regardless of where they are in the country on Election Day. While it makes sense that our electoral system is fragmented, decentralized, and locally organized, a centralized election
management board of independent election, cybersecurity, and legal experts could not only fit within our political culture, but it could also enhance it.
V. DISCUSSION

The secret ballot reform was a successful transnational movement that put aside idealistic conceptions of democracy and addressed the harsh social reality of corruption in voting systems. The effects of that transnational effort lead to the modern appreciation of the importance of voter privacy and the secret ballot. While almost all modern democracies consider the secret ballot to be an essential component of holding free and fair elections, each country has developed its own unique method of protecting voter privacy. In Estonia, the privacy concerns with remote i-Voting are mitigated by allowing voters to change their digital ballot as many times as they need and by offering voters the ability to cast their ballot at the polling site if they feel their privacy had been violated. Finland is far less flexible when it comes to voting and enforces secrecy through supervision of election officials. All voters must vote using a hand-marked paper ballot at a polling station. Only under special circumstances are voters allowed to vote by mail, which must be done in the presence of an election official who comes to the voter’s home. In Spain, the actual act of voting is far from secret, but ballots are destroyed soon after election day, erasing all voting records, unlike in the U.S. where voter rolls are highly sought after. The United Kingdom does abide by the secrecy requirement, but their vote tracing system is in conflict with principles of the secret ballot. However, the United Kingdom mitigates risk by incorporating strict procedural steps to protect the secrecy. Each of these countries has one way of conducting national elections, while the United States has many.

The goal of this paper is not to say that the United States needs to adopt Estonia’s re-voting, Finland’s mandatory secrecy, Spain’s burning of ballots, or the United Kingdom’s vote tracing system because those systems work within their own specific political cultures. Each
country’s differing geographical size and population generates a unique set of electoral needs. However, the United States could take steps to find one voting method that fits our own political culture. The current fragmented voting system creates more confusion than certainty and more holes of vulnerability than security defenses. New threats to the secrecy and security of democratic elections will continue to surface and to face them, state and local election offices need a strong, united defense rather than a thousand weak ones.

Instead of waiting for the next crisis to serve as a wake-up call, the security of voting systems needs to be addressed now. Electoral reform in the United States is hindered by two deeply entrenched cultural norms: America’s fetishization of the Constitution and technology. Both of these qualities - the reluctance to adopt comprehensive electoral law and the penchant for technology - can be seen in HAVA. After the 2000 election, HAVA not only failed to establish uniform practices across state lines, but it also misdiagnosed the problem as a technical one, rather than a political one. Technology is only as strong as the people and processes around it, and since our processes are weak, it might be best to revert to a paper-based system (Sweeney, 2018). Furthermore, cyber-attacks can never be wholly prevented; therefore, if a country wants to prevent them from happening, they should try to use as much of a paper-based system as possible. With the exception of Estonia, the majority of the European Union member-states use paper ballots not because they lack technological expertise, but because they are realistic about the limitations of technology. Until there is a voting machine that cybersecurity experts deem as suitable for elections, we should lower the risks through securing the procedures and people around the technology. David Harvey (2003) argues that often social actors “endow technology

---

22 See Figure 18. Comparison of Geography and Population.
with causative powers to the point that they will uncritically – and sometimes disastrously –
invest in it in the naive belief that it will somehow provide solutions to whatever problems they
are encountering” (p. 3). The government’s reaction after the 2000 election, ‘solving’ the
problem by funding states to buy new technology, epitomizes that naive belief.

Pilot testing is an area in which the United States can learn from Europe. There is a
reason why the United Kingdom, France, Norway, Finland, Germany, the Netherlands, Ireland,
and more have trialed electronic voting systems and decided against using them for national
elections. Even without Europe’s example, hundreds of American cybersecurity and computer
science experts reached the same conclusions, but some states continue to ignore their
precautions. There is not a disconnect between the academic community and the election
administrations; in fact, cybersecurity experts are cited in reports. For example, in Georgia the
election administration conducted a Secure, Accessible & Fair Elections (SAFE) Commission
Report (2019) in which they write:

Dr. Wenke Lee, Professor of Computer Science in the College of Computing at the Georgia Institution for
Technology, who also holds the John P. Imlay Chair in Software at Georgia Tech, strongly feels that hand-
marked paper ballots are more secure than ballots marked using ballot-marking devices. This view is also
held and was expressed to the commission by Verified Voting and numerous professors in computer science
and cybersecurity (p. 15).

Despite Dr. Lee’s warnings and all the arguments against them, the commission still
recommends buying ballot-marking devices (BMDs) at the end of their report (Georgia Secretary
of State, 2019). Until election administrations begin listening to experts, we should not expect
future elections to be free from accusations of foreign interference or domestic election
tampering. Even if the BMDs were perfectly secure, one could still expect a contentious election
in ten or so years as time takes its toll on every electronic voting machine and eventually it will
wear out and cause accusations of voter suppression, long lines, and machine failures. Election
offices need to listen to evidence from experts and form a comprehensive, scientific approach to implementing new technologies. Instead of struggling with the ever-changing cybersecurity landscape alone, they need to work together.

There are two ways to unify our decentralized electoral administration. The first is to join European democracies in creating an independent or bipartisan election management board. Members of this board could come from many different fields - law, cybersecurity, ethics, computer science, political science, and election specialists. The board could address the nation’s electoral problems at a national level by issuing reports like the U.K.’s Election Commission, establishing national standards, recommending legislation to lawmakers, and assisting the EAC. Spain serves as a great example of how a central election board can exist without abandoning local election administrations. However, Spain is a fraction of the size of the United States and does not have multiple time zones. If Spain’s system were implemented in the United States, this problem would have to be addressed to ensure that every state had equal access to the central election management body.

Better suited to our political culture is the second option: to bypass the federal government and form an interstate coalition. States have already begun to effectively amend the constitution without having actually to do so. For example, the National Popular Vote interstate compact is an agreement among states to award all their electoral votes to the candidate who wins the popular vote. If all states agree, there would no longer be the possibility for a candidate to win the Presidency without having the popular vote. This same interstate coalition could work for voting systems as well. There needs to be an agreed upon set of standards for conducting elections so that every voter has the same right to a secret ballot. For some states, this may mean
abandoning certain voting technologies and traditions. However, if all states operated under the same voting system, local administrations could share resources, like voter education campaigns, poll worker cybersecurity training, knowledge about best practices, and uniform standards would also allow for increased accountability. Standards will continuously need to be updated because elections will never stop changing, but this is a small price to pay. Had there been a such a set of standards or a formula to follow for how to conduct a recount, how to deal with machine failure, and how to mitigate poor ballot design, the 2000 election result might have been announced days rather than weeks after election day. Furthermore, a standardized voting system could have prevented the fiasco in the first place.
FIGURES

Figure 1. Optical Scan Voting Machine
*Image Courtesy of US08136729 Patent ES&S DS200*

Figure 2. Direct Recording Electronic Voting Machine: Premier/Diebold (Dominion) AccuVote
TS & TSx
*Image Courtesy of Verified Voting*
Figure 3. Model of a Voting System
<table>
<thead>
<tr>
<th>Country</th>
<th>Estonia</th>
<th>Finland</th>
<th>Spain</th>
<th>United Kingdom</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>Former Soviet State</td>
<td>Former President ousted elected lives and remained in power for 23 years</td>
<td>After 35 years of dictatorship, Spain transitioned from Franco-era to democracy</td>
<td>Long history of voting</td>
<td>Decentralization of power</td>
</tr>
<tr>
<td></td>
<td>Unique opportunity to build their technological infrastructure from scratch</td>
<td>Set to rules to control laws</td>
<td>Strong support from their party</td>
<td>Success in civil liberties</td>
<td>Success in civil liberties</td>
</tr>
<tr>
<td></td>
<td>e-Governance: convenience and efficiency</td>
<td>Ale, city, Berlin, voters in Berlin</td>
<td>UVF voting system is in effect in the United Kingdom</td>
<td>Long history of voting</td>
<td>Long history of voting</td>
</tr>
<tr>
<td></td>
<td>Digital Signature Act allows for digital signature verification of the vote during the vote and post the vote</td>
<td>Elected of 1986 are in the Finnish electoral system and to the Finnish electoral system</td>
<td>The Organic Law of the General Elections of the People and the Electoral Law of the People</td>
<td>わかめらしを制限するための法律</td>
<td>Voting Act of 2016</td>
</tr>
<tr>
<td><strong>Voting Method for Privacy</strong></td>
<td>Mail-in ballots are issued with a unique identification number during the voting process</td>
<td>Mail-in ballots are issued with a unique identification number during the voting process</td>
<td>Mail-in ballots are issued with a unique identification number during the voting process</td>
<td>Mail-in ballots are issued with a unique identification number during the voting process</td>
<td>Mail-in ballots are issued with a unique identification number during the voting process</td>
</tr>
<tr>
<td><strong>Voting Technology</strong></td>
<td>Option in remote voting system</td>
<td>Paper ballots are gridded and scanned</td>
<td>Paper ballots are printed and scanned</td>
<td>Paper ballots are printed and scanned</td>
<td>Paper ballots are printed and scanned</td>
</tr>
<tr>
<td></td>
<td>X-ray technology is used</td>
<td>Bar code scanning and such scanning machines</td>
<td>Bar code scanning and such scanning machines</td>
<td>Bar code scanning and such scanning machines</td>
<td>Bar code scanning and such scanning machines</td>
</tr>
<tr>
<td><strong>Election Administration</strong></td>
<td>National Election Committees oversees elections</td>
<td>The Ministry of justice</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
</tr>
<tr>
<td></td>
<td>The State Electoral Office (part of the NED) oversees voting</td>
<td>The Ministry of Justice</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Ministry of justice</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Ministry of justice</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
<td>Central Election Board oversees elections</td>
</tr>
</tbody>
</table>
In Estonia, you can vote with either an ID-card (a plastic national ID-card with a chip inside) or Mobile-ID (voting using a smartphone).

To authorize an ID-card, citizens need to connect it to a computer via a smart card reader.

The most popular operating system with i-Voting Estonians is Windows (92.6 percent), the second place is iOS and the third — Linux.

Estonians can vote wherever they can get internet connection. Estonia has one of the highest internet penetration rates in the world.

The voter's identity is removed from the ballot before it reaches the National Electoral Commission thereby ensuring anonymity.

A separate Electronic Voting Committee is responsible for conducting internet voting, but the National Electoral Commission retains a supervisory role.

Figure 5. i-Voting in Estonia
Image Courtesy of Stella Shabliovska, Kyiv Post/National Electoral Commission of Estonia

Figure 6. Envelope Scheme
Image Courtesy of State Electoral Service of Estonia
Figure 7. The Principle Parties of the i-Voting System
*Image Courtesy of State Electoral Service of Estonia*

Figure 8. Finland’s Experiment with Touch Screen Voting Machines
*Image Courtesy of Vaalit Val*
Figure 9. Spanish Polling Place
*Image Courtesy of Cesar Manso/AFP*

Figure 10. Example of a Ballot Paper in the United Kingdom
*Image Courtesy of ACE Project.*
Figure 11. Counting Process in the United Kingdom
*Image Courtesy of Julie Howden/EPA*

Figure 12. The Five Different Kinds of Chads
*Image Courtesy of Carter M. Yang ABC News*

Figure 13. Palm Beach’s 2000 Butterfly Ballot
*Image Courtesy of The Sun Sentinel*
Figure 14. Votomatic Voting Machine Used in the 2000 Election
Image Courtesy of Verified Voting

Across the U.S., a patchwork of voting methods
Principal voting system, by county

Source: Pew Research Center analysis of data from Verified Voting Foundation.
PEW RESEARCH CENTER

Figure 15. Patchwork of Voting Technologies Across the United States
Image Courtesy of Pew Research Center
Figure 16. Premier/Diebold AccuVote OS Optical Scan Machine  
*Image Courtesy of Verified Voting*

Figure 17. ES&S’s AutoMARK OS Ballot Marking Device  
*ImageCourtesy of Verified Voting*

<table>
<thead>
<tr>
<th>Country</th>
<th>Estonia</th>
<th>Finland</th>
<th>Spain</th>
<th>United Kingdom</th>
<th>United States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Population</td>
<td>1 million</td>
<td>5 million</td>
<td>48 million</td>
<td>65 million</td>
<td>327 million</td>
</tr>
<tr>
<td>Square Miles</td>
<td>17,462 mi²</td>
<td>130,663 mi²</td>
<td>195,363 mi²</td>
<td>93,783 mi²</td>
<td>3,796,525 mi²</td>
</tr>
<tr>
<td>Size Comparison</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

Figure 18. Comparison of Geography and Population  
*Images Courtesy of MapFight*
REFERENCES


https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it


Retrieved from: https://apnews.com/5dca86cf28114b23b94e4a3891da1d64


https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2981&context=facpub

Collin, K. (2016). Everything you need to know about election observers — and why the U.S.


https://doi.org/10.2307/2110757

http://www.jstor.org.proxy.library.georgetown.edu/stable/23014789


  
  https://e-estonia.com/solutions/e-identity/id-card/

  

  
  http://www.juntaelectoralcentral.es/cs/jec/electoralAdministration

  


Georgia Secretary of State. (2019). *Secure, Accessible & Fair Elections (SAFE) Commission*


Center for the Study of Language and Information.


https://doi.org/10.4324/9780203877111-11


https://doi.org/10.2307/1958367


https://doi.org/10.1057/9781403977212


https://doi.org/10.2139/ssrn.205449


http://www.dcs.gla.ac.uk/~tws/papers/storer05electronic.pdf


