Algorithmic Elections

Sarah M.L. Bender

University of Michigan Law School

Follow this and additional works at: https://repository.law.umich.edu/mlr

Part of the Election Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://repository.law.umich.edu/mlr/vol121/iss3/5

https://doi.org/10.36644/mlr.121.3.algorithmic

This Note is brought to you for free and open access by the Michigan Law Review at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.
NOTE

ALGORITHMIC ELECTIONS

Sarah M.L. Bender*

Artificial intelligence (AI) has entered election administration. Across the country, election officials are beginning to use AI systems to purge voter records, verify mail-in ballots, and draw district lines. Already, these technologies are having a profound effect on voting rights and democratic processes. However, they have received relatively little attention from AI experts, advocates, and policymakers. Scholars have sounded the alarm on a variety of “algorithmic harms” resulting from AI’s use in the criminal justice system, employment, healthcare, and other civil rights domains. Many of these same algorithmic harms manifest in elections and voting but have been underexplored and remain unaddressed.

This Note offers three contributions. First, it documents the various forms of “algorithmic decisionmaking” that are currently present in U.S. elections. This is the most comprehensive survey of AI’s use in elections and voting to date. Second, it explains how algorithmic harms resulting from these technologies are disenfranchising eligible voters and disrupting democratic processes. Finally, it identifies several unique characteristics of the U.S. election administration system that are likely to complicate reform efforts and must be addressed to safeguard voting rights.

TABLE OF CONTENTS

INTRODUCTION..............................................................................................490
I. ALGORITHMIC DECISIONMAKING AND ALGORITHMIC HARM S...492
   A. Key Technical Terms and Concepts...............................................493
   B. How Algorithms Harm...............................................................494
      1. Faulty Programming and Design..........................................495
      2. Faulty Uses..............................................................497
      3. Proxy Discrimination.........................................................498

* J.D. Candidate, May 2023, University of Michigan Law School. Thank you to Professors Nicholson Price and Ellen Katz for their extensive feedback, guidance, and encouragement throughout the research and writing of this piece. Thanks also to Maddie McFee, who provided comments on multiple drafts, and to members of the Student Research Roundtable. I am further grateful to the Michigan Law Review Volume 121 Notes Editors, especially Annie Schuver, for their perceptive feedback and editing. Last but not least, thank you to my family, friends, and Win for their unwavering love and support. All errors are my own.
INTRODUCTION

In recent years, the potential for algorithms to make voting easier and elections fairer and more reliable has gained increased attention. Computer scientists have developed algorithms to make redistricting less partisan, which have been touted as a cure for gerrymandering.\(^1\) Counties are using artificial intelligence technologies (AIs) to perform mobile-only elections, allowing voters to cast their ballots using a smartphone or other electronic device.\(^2\) Others are piloting algorithmic tools that track voter data to ensure that no fraud or significant administrative errors occur.\(^3\)

AI holds great promise. It can be used to automate a wide variety of processes and decisions that were previously performed by humans and are thus susceptible to error and inefficiencies. And unlike humans, algorithms cannot

---

themselves engage in intentional discrimination. As a result, they have the potential to improve traditional human decisionmaking and to render more objective and less discriminatory results.

Unfortunately, this hope has not borne out in practice. Algorithms have instead proven to be “our opinions embedded in code.” Indeed, “[m]ounting evidence reveals that algorithmic decisions can produce biased, discriminatory, and unfair outcomes in a variety of high-stakes economic spheres including employment, credit, health care, and housing.” Prejudice can infect AIs and algorithms in a variety of ways, causing them to compound existing injustices and yield discriminatory results. For example, AI-generated recidivism scores used in Florida were almost twice as likely to falsely label Black defendants as future criminals, as compared to white defendants.

Extensive scholarship has documented how AI is being used in the criminal justice, housing, education, employment, financial services, and healthcare domains, as well as the risks it poses to civil rights and civil liberties. Relatively little attention has been given to its use in U.S. elections or its impact on voting rights, however. This Note seeks to further that conversation.

This Note has two primary target audiences. The first is AI experts, legal scholars, policymakers, and advocates who are working to promote algorithmic accountability in other domains. I hope to persuade this group of the importance of addressing algorithmic harms in elections and voting—and to provide them with an initial framework for doing so effectively. The second target audience comprises public officials and voting rights advocates and experts who are working to improve our election systems but may be less familiar with AI. My goal is to provide this group with a workable understanding of how AI may affect their work, as well as why such technology must be deployed cautiously.

Part I seeks to facilitate conversation between these two audiences by providing a brief primer on the technical concepts discussed in this Note and by relating the different types of “algorithmic harms” that scholars have identified in other domains that are relevant to elections and voting. Part II is the

4. See infra note 94 and accompanying text.
9. See infra Section I.B.
10. See infra note 11 (surveying scholarly literature on AI and elections).
heart of the Note. It catalogs the different ways that election administrators use AI to make decisions and manage elections, as well as the algorithmic harms this may cause. This is the most comprehensive review of AI’s use in elections and voting to date.\footnote{11} Finally, Part III identifies several unique characteristics of election administration in the United States and explains why these characteristics may complicate efforts to address algorithmic harms in this domain.

I. ALGORITHMIC DECISIONMAKING AND ALGORITHMIC HARMs

Not all members of this Note’s target audiences are familiar with how AI and algorithms work, and some of the terms used in this Note have been defined in different ways. This Part seeks to establish a baseline understanding of how algorithmic decisionmaking\footnote{12} can produce inaccurate, biased, and unfair outcomes. Section I.A defines the key technical terms used throughout this Note, as well as the scope of the technologies discussed in Part II. Section I.B describes different types of “algorithmic harms” that are relevant to elections and summarizes existing literature on how such harms occur and manifest in other civil rights domains.

\footnote{11} Though there is a growing body of literature about AI’s use in redistricting, these pieces do not address other forms of algorithmic decisionmaking in election administration. See, e.g., Zhang, supra note 1; Rudeen, supra note 1. Similarly, other scholarship has examined the use of algorithmic technologies in voter roll maintenance or signature verification but does not address some other uses of AI in these fields and/or makes no mention of AI’s use in redistricting. See, e.g., NAT’L RSCH. COUNCIL, ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING 47–49 (Richard Celeste, Dick Thornburgh & Herbert Lin eds., 2006) (describing the use of name-matching algorithms in voter roll maintenance but not the interstate cross-checking technologies described in Section II.A); ROXANA ARJON ET AL., STANFORD L. SCH., SIGNATURE VERIFICATION AND MAIL BALLOTS 29 (2020), https://www-cdn.law.stanford.edu/wp-content/uploads/2020/04/SLS_Signature_Verification_Report-5-15-20-FINAL.pdf [perma.cc/XYN4-SQAJ] (surveying the use of signature-matching AIs but not list-maintenance or redistricting AIs in California); BRUCE YELLIN, DELL TECHS., CAN TECHNOLOGY RESHAPE AMERICA’S ELECTION SYSTEM? (2021), https://education.dell EMC.com/content/dam/dell-emc/documents/en-us/2021KS_Yellin-Can_Technology_Reshape_Americas_Election_System.pdf [perma.cc/7R63-BEE6] (describing some of the ways AI is used in voter roll maintenance, signature matching, and election interference but making no mention of redistricting technologies). A number of scholars and journalists have also called attention to AI’s use in political advertising and election interference. See, e.g., Elaine Kamarck, Malevolent Soft Power, AI, and the Threat to Democracy, BROOKINGS (Nov. 29, 2018), https://www.brookings.edu/research/malevolent-soft-power-ai-and-the-threat-to-democracy [perma.cc/VN6D-D6FY]; Jeff Berkowitz, The Evolving Role of Artificial Intelligence and Machine Learning in US Politics, CTR. FOR STRATEGIC & INT’L STUD. (Dec. 21, 2020), https://www.csis.orgblogs/technology-policy-blog/evolving-role-artificial-intelligence-and-machine-learning-us-politics [perma.cc/FX6G-R846]. However, their works do not address how election administrators are themselves leveraging AI to make decisions and manage elections.

\footnote{12} This Note uses the term “algorithmic decisionmaking” to refer to any decisionmaking or administrative process that has been automated by an algorithm or has otherwise been informed by an algorithmic system’s results.
A. Key Technical Terms and Concepts

This Note uses a variety of terms to refer to the emerging technologies revolutionizing election administration and other domains. These include “algorithms,” “artificial intelligence,” and “machine learning.” Some authors have used the image of a Russian nesting doll to illustrate the relations between these terms—algorithms are the largest, outermost doll because, while all AI uses algorithms, not all algorithms constitute AI. Similarly, all machine learning involves AI, but not all AI involves machine learning.

Broadly speaking, an algorithm is “a finite series of well-defined, computer-implementable instructions” used to process input data and generate certain outputs. Today, nearly all software programs use some type of algorithm to solve problems and execute tasks. Algorithms can be quite simple, like generating a Fibonacci sequence. They can also be quite complex, like those that provide autonomous vehicles with driving instructions, identify abnormal X-rays and CT scans, or assign students to public schools.

Experts define AI in a variety of ways, but the term generally refers to machines that mimic human intelligence. AI systems use algorithms to analyze text, data, images, and other inputs and make decisions about them in a way that is consistent with human decisionmaking. AI’s “ability to extract intelligence from unstructured data” is particularly impactful. Vast amounts of data are generated daily, which, on their face, have little apparent meaning. The goal of AI is to make sense of such data, identifying new patterns and determining how best to act upon them.

14. Slaughter, supra note 7, 2 n.1.
15. Id.; The Definitive Glossary of Higher Mathematical Jargon, MATH VAULT, https://math-vault.ca/math-glossary/#algo [perma.cc/VQ78-7W63].
19. Allen & West, supra note 17.
22. Manheim & Kaplan, supra note 8, at 108.
23. Id.
24. Id.
Machine learning is a form of AI, which relies on algorithms that can learn from data without rules-based programming. These learning algorithms can “classify data, pictures, text, or objects without detailed instruction and . . . learn in the process so that new pictures or objects can be accurately identified based on that learned information.” Machine-learning technologies thus depend less on human programming and more on algorithms that can learn from data as they progress, improving at tasks with experience.

Scientists “train” machine-learning algorithms to do particular tasks by feeding the algorithm data for which the “target variable,” or outcome of interest, is known. The algorithm derives from these data “complex statistical models linking the input data with which it has been provided to predictions about the target variable.” For example, to train an algorithm to identify malignant tumors, scientists will show it a large number of tumor X-rays or scans and indicate which are benign and which are cancerous. The algorithm will begin to pick up on patterns in the tumor images, allowing it to distinguish between benign and malignant tumors in new images. Thus, the data used to train machine-learning algorithms—and the process by which scientists label the data—have a significant impact on the outcomes they generate.

B. How Algorithms Harm

Because AIs do not have any conscious awareness or intentions that are independent from those embedded within their code, “most commentators and courts believe that an AI cannot itself engage in intentional discrimination.” Nevertheless, algorithmic decisionmaking can lead to a number of harmful outcomes, which are well documented in other civil rights domains and are likewise present in election administration. Faulty training and poor design can cause algorithmic systems to render inaccurate and biased results. But even well-designed AIs may be misused or may “proxy discriminate.” Finally, these technologies’ opacity and complexity can exacerbate each of these issues by making them harder to identify and mitigate.

25. Allen & West, supra note 17.
26. Id.
29. Prince & Schwarz, supra note 27, at 1274.
31. Id.
32. See Raub, supra note 6, at 533–34.
33. Prince & Schwarz, supra note 27, at 1274.
1. Faulty Programming and Design

Though AIs have a veneer of impartiality and accuracy, each of their technical components involves human judgment. Humans select the data used to train algorithms, label these data sets, and design and program the logical steps that the algorithmic system operationalizes. Human error and bias can infect AIs and algorithms at each of these stages, which can cause them to render inaccurate and discriminatory results. These results may then be used to make high-stakes decisions, like how to allocate a limited supply of COVID-19 vaccines or whether to initiate a child welfare intervention.

“Faulty training data” is a common cause of this type of algorithmic harm. As described above, the accuracy of a machine-learning algorithm is directly linked to the quality of the data used to train it. Training data can be skewed in a variety of ways, all of which may impair the algorithm’s results and produce problematic outcomes.

First, training data may not represent the population they are designed to serve, causing biased and ungeneralizable outcomes. For example, Amazon recently discontinued its use of a recruiting AI after it found the tool was systematically discriminating against female candidates. The data used to train the AI were sourced from resumes submitted to Amazon—where men comprise 60 percent of the workforce and 74 percent of managerial positions—and benchmarked against the company’s engineers. Despite the company’s best efforts, the hiring system kept attempting to reproduce the training data’s male-heavy pattern, even penalizing resumes that included the word “women’s,” as well as the resumes of applicants who attended women’s colleges.

35. Id.
36. Slaughter, supra note 7, at 4.
38. See supra notes 28–32 and accompanying text; Slaughter, supra note 7, at 7; Solon Barocas & Andrew D. Selbst, Big Data’s Disparate Impact, 104 CALIF. L. REV. 671, 680–81 (2016).
39. Slaughter, supra note 7, at 7–8.
40. Id. at 14; Barocas & Selbst, supra note 38, at 684–87.
42. Lee et al., supra note 41.
43. Id.
Training data may also be incomplete or incorrect, which can cause the AI to render inaccurate results.\textsuperscript{44} For example, racial and ethnic minorities and low-income individuals often have missing and incorrect information in their medical records.\textsuperscript{45} Thus, algorithms trained using medical records may fail to identify significant variables and perform worse for such patients and, generally, across the board.\textsuperscript{46}

However, even AIs trained on accurate and fully representative datasets can yield unjust results.\textsuperscript{47} Historic and systemic discrimination leaves some people with “fewer skills, less wealth, poorer health and other traits that states, employers, lenders or others are interested in.”\textsuperscript{48} Even when data regarding such traits are perfectly accurate, they will reflect the injustices that caused such disparities.\textsuperscript{49} For example, policymakers may allocate more funding to schools in wealthy neighborhoods than to those in poor neighborhoods. If educational quality depends in part on such funds, then children in poor neighborhoods may fare worse on various metrics regarding educational attainment and workforce preparation.\textsuperscript{50} Data regarding such traits, however accurate, will reflect these disparities.\textsuperscript{51} In turn, AIs trained on such data may learn to reinforce these historical patterns, rendering outcomes that disfavor certain populations and compound these past injustices.\textsuperscript{52}

Programmers’ biases may also infect machine-learning algorithms through “faulty labeling” of training data. Labels instruct algorithms how to distinguish between certain inputs.\textsuperscript{53} These labels are often objective (e.g., whether an item is red or blue), but they may also entail more subjective judgment calls, like what makes a good employee.\textsuperscript{54} When one considers the severe lack of diversity in the tech industry—which is “predominantly white, Asian, and male”\textsuperscript{55}—it becomes easy to see how programmers’ biases can become embedded in these technologies.
Developers of AI systems may rely on faulty experimental design when evaluating the accuracy of their systems. This may also cause algorithmic systems to render inaccurate or misleading results. For example, developers of “affect recognition” AIs claim they can detect personality and character traits by analyzing body language, speech patterns, facial expressions, and other mannerisms. Though numerous studies have concluded that efforts to deduce individuals’ internal states based on their facial movements alone are “at best incomplete and at worst entirely lack validity,” companies continue to sell these technologies and market them as reliable predictors of social outcomes like job performance.

2. Faulty Uses

Even the most accurate and well-designed algorithmic technologies can lead to harmful results through “faulty use.” Faulty use occurs when users misinterpret the outputs of algorithmic systems. A common example is when users place too much stock in the system’s results, a phenomenon commonly referred to as “automation bias.” Despite their imperfections, AI and algorithmic technologies are shrouded in a “veneer of objectivity.” Humans tend to view automated systems as fairer and more reliable than humans. Coupled with our natural tendency “to seek out paths of least cognitive effort, [and] to expend less energy when part of a team,” this often causes AI users to overrely on and have too much confidence in these systems’ results. The risks of automation bias are greatest when AIs are marketed as producing reliable, objective results but are in fact infected with biases or other inaccuracies. However, automation bias can cause users of even the most responsibly designed AI to overgeneralize and excessively depend on its results. This can have serious and even life-threatening consequences.

56. Slaughter, supra note 7, at 10, 13.
57. Id. at 11–12.
59. Slaughter, supra note 7, at 12.
60. See Won, supra note 34, at 162.
64. Id. at 128.
65. See Slaughter, supra note 7, at 13–14.
66. See Vagle, supra note 63, at 129–30; see also, e.g., M.L. Cummings, Automation Bias in Intelligent Time Critical Decision Support Systems, in AIAA 1ST INTELLIGENT SYSTEMS TECHNICAL CONFERENCE 5 (2004), https://doi.org/10.2514/6.2004-6513 (listing several examples of automation bias “in the ‘real world’ where the consequences were deadly”).
Humans can also misuse AIs by feeding them “faulty inputs,” or input data that are low in quality or discordant with the systems’ intended use. For example, during the COVID-19 pandemic, some hospitals hurriedly repurposed AI systems that were designed and trained for non-pandemic uses and situations. Though these AIs may perform the tasks for which they were designed well, repurposing them can create a mismatch between the training data and input data, resulting in unreliable outputs. Nevertheless, hospitals have used these tools to handle highly sensitive pandemic-response tasks, like forecasting whether an infected patient might need intensive care or a ventilator.

“Contextual bias” is a related form of faulty use. It “arises in the process of translating algorithms from one context to another” (e.g., from a high-resource hospital like Memorial Sloan Kettering to a low-resource rural health center). While an AI trained in one setting may be untinged by problematic bias when deployed in the same and similar contexts, it may render biased results in other contexts if it was not trained to account for such differences.

3. Proxy Discrimination

Algorithmic systems may also “proxy discriminate.” Proxy discrimination occurs “when a facially-neutral trait is utilized as a stand-in—or proxy—for a protected trait,” like race, sex, or disability status. For example, Facebook “likes” and social media activity can accurately predict a wide range of personal characteristics, including gender, sexual orientation, race, ethnicity, religious beliefs, political views, relationship status, intelligence, use of addictive substances, and even the marital status of one’s parents. Discriminators can use these kinds of data in facially neutral ways, which nevertheless leads to differing treatment of protected classes. This can occur both intentionally and inadvertently. In either instance, the usefulness of the neutral practice
Algorithmic Elections

“derives, at least in part, from the very fact that it produces a disparate impact” and “often result[s] in disparate treatment of or disparate impact on protected classes for certain economic, social, and civic opportunities.”

Proxy discrimination demonstrates why prohibiting the inclusion of protected traits in AI models does little to mitigate algorithmic bias. For example, an AI that prices life insurance policies may begin to charge more for individuals who are members of a Facebook group focused on increasing access to testing for BRCA genetic variants, which are highly predictive of certain cancers. Members of this group are likely to have a family connection to these BRCA-related cancers and are thus more likely to be at risk themselves. Thus, even if this AI explicitly excludes genetic information from its model to comply with state law, it could still use the Facebook data to proxy discriminate against individuals with certain genetic predispositions.

4. Lack of Transparency

Transparency could help to mitigate concerns regarding algorithms’ accuracy and bias and encourage more responsible use of automated technologies. However, many AI models are shrouded by trade secret protections. These protections make it much more difficult to validate AIs’ results and to assess their accuracy and fairness.

This issue manifests in the criminal justice space, where algorithmic technologies have been used to interpret DNA evidence, fingerprint matches, and breathalyzer results in criminal convictions. The private companies that develop these tools have claimed that their algorithms are proprietary and must be kept secret to recoup their investments. But, “[w]ithout access to the details of the computerized algorithms providing incriminating evidence against

---

78. Prince & Schwarcz, supra note 27, at 1257.
79. Slaughter, supra note 7, at 20.
81. Id.
82. For example, Florida “has enacted a genetic privacy law that prohibits life insurance companies from canceling, limiting or denying coverage and from setting different premium rates based on genetic information.” Cameron Huddleston & Jason Metz, Can Life Insurance Companies Get Your Genetic Test Results?, FORBES ADVISOR (Oct. 28, 2022, 10:53 AM), https://www.forbes.com/advisor/life-insurance/genetic-testing [perma.cc/23HS-GRQ2].
85. See id. at 64.
87. Ryan, supra note 84, at 64; see also Justin Jouvenal, A Secret Algorithm Is Transforming DNA Evidence. This Defendant Could Be the First to Scrutinize It, WASH. POST (July 13, 2021,
them, . . . defendants lack the opportunity to challenge this incriminating evidence that poses real questions of accuracy, not to mention bias.”

Even when AI models and algorithms are public, their reasoning processes are often impossible to understand. Many learning algorithms, such as neural networks, constantly adapt their models to new inputs. As a result, AI programmers, users, and AIs themselves are often unable to explain how or why these “black box” algorithms reached certain conclusions. As one expert has explained, “[i]t is like asking a turtle why its species decided to grow a shell. We know it was adaptive, but may not know the precise pathway taken to reach its current state.”

This hidden decisionmaking not only makes it difficult to assess whether and why an algorithmic system is inaccurate or biased but also complicates civil rights enforcement. Much of antidiscrimination law requires a showing of intentional discrimination, not just disparate impact. For example, the “requirement of purpose” doctrine “reads an intentionality requirement into the Equal Protection Clause,” meaning actions that cause discriminatory results are only unconstitutional if the discrimination is intended. However, because AIs “do not have any conscious awareness or objectives that are independent from those that are embedded within their code,” most scholars agree that they cannot themselves engage in intentional discrimination. The organizations and individuals who adopt and use AIs certainly can. But, in many of the civil rights domains in which algorithmic harms have been examined, AIs are not adopted out of malice but rather to promote

8:00 AM), https://www.washingtonpost.com/local/legal-issues/trueallele-software-dna-courts/2021/07/12/66d27c44-6c9d-11eb-9f80-3d7646ce1bc0_story.html [perma.cc/SX3L-4PL3].
89. Manheim & Kaplan, supra note 8, at 152–53.
90. Id.; see also Prince & Schwarcz, supra note 27, at 1304.
91. Manheim & Kaplan, supra note 8, at 154.
92. See id. at 152–53.
93. Id. at 153 (citing Washington v. Davis, 426 U.S. 229 (1976)).
efficiency and cost savings. As a result, algorithmic decisionmaking may be beyond the reach of equal protection doctrine regardless of how biased it is.

II. AUTOMATING ELECTION ADMINISTRATION

Activists and experts have raised concerns about the use of AI to predict where crimes are likely to occur. They likewise worry about the use of AI to allocate police resources, assess the risk of recidivism to determine sentencing, and identify and find suspects using photos and videos. Advocates have also sounded the alarm on algorithmic bias in consumer lending, housing, education, employment, healthcare, and the allocation of government services and benefits.

95. See Darrell M. West & John R. Allen, How Artificial Intelligence Is Transforming the World, BROOKINGS (Apr. 24, 2018), https://www.brookings.edu/research/how-artificial-intelligence-is-transforming-the-world [perma.cc/K3PN-GPQX] (describing how AI is being used in criminal justice, health care, and other domains with the goal of improving decisionmaking); Hoffman & Podgurski, supra note 28, at 31 (“Most if not all medical AI algorithm developers are well-intentioned and strive in good faith to improve human health through their work.”); Shannen Balogh & Carter Johnson, AI Can Help Reduce Inequity in Credit Access, but Banks Will Have To Trade Off Fairness for Accuracy—for Now, BUS. INSIDER (June 30, 2021, 9:30 AM), https://www.businessinsider.com/ai-lending-risks-opportunities-credit-decisioning-data-inequality-2021-6 [perma.cc/PW7W-GPTV] (explaining how financial firms are turning to AI “to make faster, more efficient credit decisions” and “more accurate predictions of [] consumers’ creditworthiness, regardless of factors like race and sex”).

96. Manheim & Kaplan, supra note 8, at 153; Bathaee, supra note 94, at 920–21.


99. See FERGUSON, supra note 97, at 35–40.


103. See, e.g., Raub, supra note 6; Barocas & Selbst, supra note 38, at 684–87; Miranda Bogen, All the Ways Hiring Algorithms Can Introduce Bias, HARV. BUS. REV. (May 6, 2019), https://hbr.org/2019/05/all-the-ways-hiring-algorithms-can-introduce-bias [perma.cc/AW83-ANG5].

104. See, e.g., Hoffman & Podgurski, supra note 28; Price, supra note 71.

105. See, e.g., AI NOW, supra note 37, at 7, 14.
Relatively little attention has been paid to AI’s use in elections and its impact on voting rights. Election officials have begun to leverage intelligent computing technologies to streamline a variety of election administration activities, including voter roll maintenance, signature matching, and redistricting. As in other domains, AI has the potential to make these processes more efficient, equitable, and accessible. But these technologies also raise the same aforementioned concerns regarding accuracy, fairness, and transparency.

This Part provides the most comprehensive review to date of how algorithmic technologies are being used in U.S. election administration and the risks they pose to voting rights and election integrity. Section II.A describes the use of AI in voter roll maintenance, including voter purges. Section II.B focuses on signature-matching AIs, which many states use to validate mail-in ballots. Section II.C explores algorithmic technologies’ current and future impact on redistricting, including the effects of the Supreme Court’s recent decision in *Rucho v. Common Cause*. Finally, Section II.D briefly describes several AI developments that are related to elections and voting but fall outside of the election administration domain.

### A. Maintaining Voter Rolls

The Help America Vote Act of 2002 (HAVA) requires states to create, for use in federal elections, a “single, uniform, official, centralized, interactive computerized statewide voter registration list,” containing registration information and identifying every registered voter in the state. States cannot satisfy this requirement if their cities and counties maintain their own voter registration systems; HAVA requires “a true statewide system that is both uniform in each local election jurisdiction and administered at the state level.” After a voter registry is created, states must keep ineligible voters off the registration lists and add newly registered voters to them.

The practice of removing voters from these lists is commonly referred to as “voter purging.” Voters can lose their eligibility for a variety of reasons, including changes in residence, felony convictions, mental incapacity findings, death, or inactivity. List maintenance is important for both election

---

106. See, e.g., id. (reviewing recent scholarship on algorithmic accountability related to healthcare, criminal justice, education, public benefits, and immigration but making no mention of elections or voting).
107. See infra Sections II.A–C.
108. See supra Section I.B.
111. NAT’L RSCC. COUNCIL, supra note 11, at 46.
112. Id.
113. See, e.g., id.
114. Id.
integrity and efficiency; experts estimate that one in every eight registrations is invalid, which can increase the risk of voter fraud and clog voter rolls.\textsuperscript{115}

However, voter purges are also prone to error. For example, in 2016, Arkansas removed from the state’s voter rolls more than 50,000 people who were purportedly ineligible to vote because they had been convicted of a felony.\textsuperscript{116} The purge list was extremely inaccurate: at least 4,000 people did not have a disqualifying conviction, and up to 60 percent of those who did have disqualifying convictions were eligible to vote because their voting rights had been restored.\textsuperscript{117} These types of errors can “reduce confidence in the voting process, exclude voters from certain forms of official election communication, and result in disenfranchisement if a citizen is removed and does not reregister before their state’s registration deadline.”\textsuperscript{118} Voter purges can also be used to manipulate election outcomes\textsuperscript{119} and to discriminate against poor and minority voters.\textsuperscript{120} Though the National Voter Registration Act (NVRA)\textsuperscript{121} set federal standards for voter purges in 1993, states continue to conduct illegal purges and adopt policies that violate the NVRA.\textsuperscript{122}

Because voter registration lists generally contain millions of entries, purges must be at least partially automated.\textsuperscript{123} To achieve this, computers compare voter registration lists with information from other sources, such as death notices, felony conviction records, and recent address lists, to determine who remains eligible.\textsuperscript{124} This task can be even more complicated than it seems. The same individual may be listed differently across various databases. For example, “John Jones and John X. Jones may refer to the same person, and he may have given the former name in registering to vote and the latter name in

\begin{itemize}
  \item \textsuperscript{115} Gregory A. Huber, Marc Meredith, Michael Morse & Katie Steele, \textit{The Racial Burden of Voter List Maintenance Errors: Evidence from Wisconsin’s Supplemental Movers Poll Books}, SCI. ADVANCES, Feb. 17, 2021, at 1.
  \item \textsuperscript{117} Id.
  \item \textsuperscript{118} Huber et al., supra note 115, at 1.
  \item \textsuperscript{119} Nat’l Rsch. Council, supra note 11, at 49.
  \item \textsuperscript{121} 52 U.S.C. §§ 20501–20511.
  \item \textsuperscript{122} Brater et al., supra note 120, at 1–2.
  \item \textsuperscript{123} Nat’l Rsch. Council, supra note 11, at 46.
  \item \textsuperscript{124} Id.
\end{itemize}
obtaining a driver’s license.” The same name may also refer to many different people, or names may be misspelled. Name-matching algorithms are widely used to overcome these challenges.

It is particularly difficult to update voter lists when people move between states. There is no central body in the United States to monitor when people move from one state to another, and, in general, there is no requirement for registered voters to cancel their registrations before moving. As a result, roughly 2.75 million Americans were on more than one state’s voter rolls as of 2012.

Interstate cross-checking became feasible after states began to centralize, standardize, and digitize their voter rolls in 2002 as part of HAVA. Since then, states have experimented with algorithmic decision systems to exchange voter data. In 2005, the Kansas Secretary of State launched the Interstate Voter Registration Crosscheck Program (“Crosscheck”), a data-matching system that purported to root out voter fraud. Crosscheck worked by comparing states’ voter files and sending participating states a list of voter registrations that matched those of another state. Though states could use this information however they wished, Crosscheck provided guidelines for purging these voters’ records.

Another interstate cross-checking initiative has since taken hold. A non-profit organization called the Electronic Registration Information Center (ERIC) uses algorithm processes to assist thirty states and the District of Columbia in identifying unregistered individuals and maintaining accurate voter registries. ERIC generates two types of lists for member states: (1) lists

125. Id. at 47.
126. Id.
127. Id. at 48.
129. Id.
130. Id. at 26.
131. Id.
133. Ingraham, supra note 132.
135. Huber et al., supra note 115, at 1; see also ELEC. REGISTRATION INFO. CTR., Ensuring the Efficiency and Integrity of America’s Voter Rolls, https://ericstates.org [perma.cc/NVL9-D5VZ].
of residents who are likely to be eligible to vote but are not registered, and (2) lists of registrants who may have moved, died, or have duplicate registrations. Member states agree to contact the individuals on these lists, often using a mailed postcard, to either encourage them to register or to confirm that their registrations are accurate.

Though such algorithmic systems can help to streamline a cumbersome and difficult administrative task, they pose a number of potential algorithmic harms. First, they may render biased, inaccurate results, which can disenfranchise eligible voters. For example, at least one study has found that name-matching algorithms’ accuracy varies among racial and ethnic groups. Specifically, these tools rendered more “mismatches” for Asian names.

Similar concerns about accuracy and bias have been raised regarding interstate cross-checking systems. Crosscheck was suspended in 2019 as part of a settlement with the ACLU of Kansas after researchers found that the tool was overrun with security flaws and false positives. For every duplicate registration that the tool accurately identified and eliminated, the tool incorrectly flagged roughly 200 registrations that were used to cast legitimate votes. These voter records were purged, jeopardizing these eligible voters’ ability to cast a ballot.

ERIC has raised fewer civil rights concerns than Crosscheck and has even enabled some member states to increase voter registration rates through outreach to individuals who are eligible to vote but not on their voter rolls. However, because its lists are also used in states’ voter purges, it has the

---

137. Id. at 1.
139. Id.
143. See id.
145. Huber et al., supra note 115, at 1.
same capacity for voter disenfranchisement. But, as Justice Breyer noted in his dissent in *Husted v. A. Philip Randolph Institute*, “more often than not, the State fails to receive anything back from the registrant.” Individuals may fail to confirm their eligibility for a variety of reasons, including recipients suspecting that the postcards sent by states to confirm their registration are junk mail or a scam or simply never receiving them. Whatever the cause, individuals who fail to respond to states’ outreach may be purged from voter rolls, leaving them unable to vote in the next election.

Despite ERIC’s impact on an important matter of public concern, there has been little transparency regarding its processes and outcomes. As a result, assessing its accuracy and potential discriminatory impact is difficult. Internal evaluations of ERIC’s list-maintenance practices have not been publicly released, and independent external reviews have not occurred because ERIC’s Membership Agreement prevents states from disclosing ERIC data to third parties. At least one study, however, has found that minority voters are more likely to be incorrectly removed from voter files because of ERIC’s lists.

Even a well-designed algorithmic system will yield inaccurate results if its users input data that are unrelated to the system’s target variable. This type of “faulty input” has fueled voter purges in the past. For example, election officials in some states used the federal government’s Systematic Alien Verification for Entitlements (SAVE) database to compile voter purge lists. But SAVE was not designed for this purpose; it is meant to verify immigration status to determine eligibility for public benefits and, thus, includes data concerning both citizens and noncitizens. Still, some states relied on the SAVE list as a way to verify the citizenship status of registered voters, eliminating the records of those they concluded were noncitizens. Using SAVE in this way risked disenfranchising eligible voters, particularly those who had recently become naturalized citizens. This practice was challenged, and, in 2014, the

---

146. *See id.* at 2.
147. *Id.*
149. *Id.*
150. *Id.*
152. *Id.* at 7–8.
156. *Id.* at 68; *see also* Hu, *supra* note 153, at 683–84.
Eleventh Circuit found it to violate the NVRA for this reason.\textsuperscript{157} Nevertheless, other faulty inputs could be used in the future.

Concerns about the accuracy and bias of voter purges are neither new nor unique to algorithmic systems. Nevertheless, these systems merit special attention for several reasons. First is the risk of automation bias. Purge lists generated by algorithmic systems may appear more objective and accurate, and thus may be subject to less scrutiny by election administrators, lawmakers, and the general public.

Further, incorporating complex algorithms into the list-maintenance process could make it harder to ensure that states and officials are complying with the NVRA and other laws governing voter purges. Ensuring compliance is difficult even with traditional forms of list maintenance.\textsuperscript{158} AI will likely further complicate oversight and enforcement efforts by making these processes even less transparent.

B. Signature Matching

A record number of voters cast their ballots by mail during the 2020 elections.\textsuperscript{159} Before the vast majority of these votes were counted, they underwent a signature-matching test.\textsuperscript{160} As of 2020, thirty-three states required validation of voters’ signatures on mail-in ballots.\textsuperscript{161} In the 2016 elections, signature discrepancies were the most common reason for rejecting mail-in ballots,\textsuperscript{162} and, over the course of the 2016 and 2018 elections, more than 750,000 absentee ballots were voided during the signature-matching process.\textsuperscript{163}

The signature-verification process varies dramatically between states and even from county to county.\textsuperscript{164} Election officials adhere to a wide variety of rules and procedures and receive little, if any, training about how to identify fraudulent signatures.\textsuperscript{165} Whatever the process, signature verification can be

\textsuperscript{157.} Arcia v. Fla. Sec’y of State, 772 F.3d 1335, 1348 (11th Cir. 2014).
\textsuperscript{158.} See BRATER ET AL., supra note 120.
\textsuperscript{161.} Id.
\textsuperscript{162.} Ben-Achour, supra note 159.
\textsuperscript{163.} Wiggers, supra note 160.
\textsuperscript{165.} Id.
extremely burdensome for election officials who must deliver speedy results with limited staff.166

As a result, many jurisdictions have begun using AI to automate the signature-verification process.167 At least twenty-nine counties in eight states,168 all or most of which are in the top hundred largest counties by registered voters,169 use signature-matching software. This software uses machine learning to compare signatures found on mail-in ballots with those in voters’ files.170 Algorithms evaluate certain features of these signatures, like their width, height, symmetry, and stroke directions to identify points of similarity.171 If the signature clears a fixed “confidence threshold,” the ballot is marked as verified; if not, it is flagged as a possible mismatch.172

Though jurisdictions use a variety of machines to process mail-in ballots,173 most counties use the same signature-matching software created by Parascript.174 The similarities end there. Counties leverage this software in dramatically different ways. First, jurisdictions have different rules about what comparison signatures the algorithms can use to verify the ballot. Most allow the software to access all of the signatures in voter files, including those from departments of motor vehicles (DMVs).175 However, other counties restrict the machines to use only voters’ original voter registration signatures.176

Second, officials can set different confidence thresholds for verifying signatures.177 As a result, ballots with the same number of points of similarity could be approved in one jurisdiction but flagged as a mismatch in another. This can dramatically affect ballot approval rates.178

Third, jurisdictions have different procedures for how they use the software’s results. In many jurisdictions, ballots flagged as a possible mismatch


167. E.g., Ben-Achour, supra note 159; Wiggers, supra note 160; Dave & Sullivan, supra note 166; YELLIN, supra note 11, at 17–18.

168. Ben-Achour, supra note 159.

169. Dave & Sullivan, supra note 166.


171. Wiggers, supra note 160; ARJON ET AL., supra note 11, at 26–29.

172. ARJON ET AL., supra note 11, at 29.

173. Id. at 30.

174. Dave & Sullivan, supra note 166; Wiggers, supra note 160.

175. Ben-Achour, supra note 159.

176. ARJON ET AL., supra note 11, at 23.

177. Wiggers, supra note 160.

178. Id.
are manually examined by staff, while those the AI approves are not.\textsuperscript{179} Other counties require staff to verify each ballot, regardless of the AI’s results.\textsuperscript{180}

Many experts worry that these signature-matching AIs are flagging the wrong ballots, with marginalized voters bearing the brunt of such errors. Though studies have reached conflicting conclusions regarding these programs’ accuracy, some estimate that it could be as low as 74 percent.\textsuperscript{181}

“Faulty training data” is one cause of these tools’ inaccuracies. These algorithms are trained on unrepresentative datasets and thus may continue to disadvantage certain groups of voters.\textsuperscript{182} For example, existing signature-matching software programs are often trained only on English handwriting.\textsuperscript{183} As a result, voters who do not write in English may be at a greater risk of having their ballot rejected.\textsuperscript{184}

Because manual signature matching processes are also highly inaccurate and tend to disfavor certain groups of voters, similar disparities could result if AIs are trained on historical datasets. As previously noted, election officials who verify signatures receive little to no training, increasing the likelihood that they will flag a genuine signature as a fake.\textsuperscript{185} Further, studies have repeatedly found that young voters,\textsuperscript{186} elderly voters,\textsuperscript{187} voters with disabilities,\textsuperscript{188} voters of color,\textsuperscript{189} and first-time mail-in voters\textsuperscript{190} experience higher rejection rates. Those who have changed their name are also at a disadvantage, meaning that “married women, trans people, or domestic abuse survivors [are] disproportionately likely to have their vote cast out.”\textsuperscript{191}

“Faulty inputs” may also be to blame. These technologies are often used to compare ballots, which are signed by hand on paper, with those collected

\textsuperscript{179} ARJON ET AL., supra note 11, at 23.
\textsuperscript{180} Id.
\textsuperscript{181} Wiggers, supra note 160.
\textsuperscript{182} Ben-Achour, supra note 159.
\textsuperscript{183} Wiggers, supra note 160.
\textsuperscript{184} Id.
\textsuperscript{186} See id.; Graham, supra note 164.
\textsuperscript{187} Lau & Nelson, supra note 185; Graham, supra note 164; see also Lila Carpenter, Signature Match Laws Disproportionately Impact Voters Already on the Margins, ACLU (Nov. 2, 2018, 2:45 PM), https://www.aclu.org/blog/voting-rights/signature-match-laws-disproportionately-impact-voters-already-margins [perma.cc/3GNG-Y3U5].
\textsuperscript{188} Carpenter, supra note 187; Lau & Nelson, supra note 185; Graham, supra note 164.
\textsuperscript{189} See Lau & Nelson, supra note 185; Wiggers, supra note 160.
\textsuperscript{190} Lau & Nelson, supra note 185; Graham, supra note 164.
\textsuperscript{191} Wiggers, supra note 160; see also Carpenter, supra note 187.
on electronic signature pads at DMVs. 192 These electronic pads tend to produce low-quality images of voters’ signatures. 193 People also move their hands differently when signing on an electronic pad, 194 and, because they do not know that their DMV signatures could be used to verify future ballots, may not put much care into those signatures. 195 As a result, the signatures on which these software programs rely often look like “scribble,” 196 which can contribute to the software’s inaccuracies.

Whatever the cause, these inaccuracies often result in eligible voters’ disenfranchisement. Only eighteen states require officials to notify voters when signature mismatches cause their ballots to be rejected. 197 But even in these states, many voters are left unaware that their signatures and ballots were rejected, and thus are left disenfranchised. 198

Despite these technologies’ potentially harmful impact on voting rights, the algorithms upon which they rely are often not available for public use or verification. 199 Their use is also largely unregulated. Federal and state laws that regulate the use of electronic voting systems do not extend to automated scanners, like those used to verify voter signatures. 200 Though the U.S. Election Assistance Commission has said that “software should be set only to accept nearly perfect signature matches and that humans should double-check a sample,” it has not provided states with concrete guidance on acceptable error rates or sample sizes, nor does it require signature-matching software vendors to publish their error rates. 201

C. Redistricting

Algorithmic systems have already upended how redistricting and gerrymandering occur. 202 While historical efforts relied on guesswork, today’s mapmakers have access to expansive yet highly granular voter data sets and advanced data analytics. 203 When taken together, redistricting software can

---

192. Ben-Achour, supra note 159.
194. See Ben-Achour, supra note 159.
196. Id.
197. Ben-Achour, supra note 159.
198. Wiggers, supra note 160; Ben-Achour, supra note 159.
199. Wiggers, supra note 160.
200. ARJON ET AL., supra note 11, at 29.
201. Wiggers, supra note 160.
203. Id.; see also Brief of Amici Curiae Political Science Professors in Support of Appellees and Affirmance at 20–22, Rucho, 139 S. Ct. 2484 (No. 18–422) [hereinafter Political Science Professors Brief].
generate tens of thousands of hypothetical district maps and precisely forecast how each would affect either political party’s electoral chances.\footnote{204}

Experts have raised concerns about these technologies, which they argue are imbued with partisan bias.\footnote{205} However, the Supreme Court has set few limits on their use (or on partisan and racial gerrymandering more broadly).\footnote{206} The Court had the opportunity to address the redistricting software’s use in \textit{Rucho v. Common Cause} but instead held that partisan gerrymandering claims are nonjusticiable\footnote{207} and left the issue to state courts and legislatures.\footnote{208}

This decision has paved the way for even more sophisticated technologies, like AI, to infect redistricting processes.\footnote{209} Though much attention has been given to AI’s potential to make redistricting less partisan,\footnote{210} it is also “uniquely suited to perpetrate gerrymanders in ways that computer systems would not have been able to during the 2010 redistricting cycle.”\footnote{211} Machine-learning technologies outperform current redistricting tools, which still struggle to capture nonlinear and context-dependent voting behavior.\footnote{212} In contrast, AI tools can identify new patterns and predictive variables,\footnote{213} allowing mapmakers to predict voting behavior at the individual level and create maps that are heavily gerrymandered but technically comply with existing legal standards.\footnote{214} The improved predictive power provided by AI tools has the ability to bolster other statistical techniques. For example, a redistricting technique called “matched-slice” gerrymandering uses individualized voting patterns to identify an opposing party’s most reliable voters and then draw maps that will neutralize them.\footnote{215} Though this technology was not yet ready to be deployed in past redistricting cycles, it is expected to be used in the near future.\footnote{216}

There is also a clear risk of “proxy discrimination” in this domain. Even AIs that lack specific data about voters’ party registration or race can “search...
out latent or discrete statistical characteristics among groups of likely voters that would correlate with them voting for a particular party, or [are] suggestive of their belonging to given racial groups.”

Though federal law more clearly prohibits racial gerrymandering, guidance on the issue remains murky. Further, partisanship and race are closely connected in many parts of the country, making racial and partisan gerrymanders “increasingly difficult to tease apart.” Thus, mapmakers could always claim that their motivations—and the AI’s goals—were purely partisan, not racial, and thus nonjusticiable under *Rucho*.

Though this type of proxy discrimination is not a new problem, AI amplifies the risk in several ways. First, AIs may proxy discriminate *accidentally*. If membership in a protected class is correlated with a neutral target variable, an AI trained to seek out this target variable may, inadvertently, end up favoring or disfavoring members of that group.

AI may also make it harder to rectify instances of proxy discrimination. Because of the “obscur[ed] visibility into both the inputs and the formulae used to make . . . decisions,” AI may make it harder to determine when such bias is occurring. Even where human actors are deploying AIs that proxy discriminate intentionally, the opacity of these technologies may conceal their biased decisionmaking, shielding them from accountability and oversight. This can increase such tools’ “appearance of impartiality” and thus also the risk of automation bias.

### D. Other Potentially Impactful AI Developments

There are other uses of AI which, while related to elections and voting, do not directly affect how election administrators manage and make decisions.
about elections. This Note will not explore these in depth. However, a few merit brief mention.

1. Political Advertising

First, AI is dramatically reshaping advertising, including political advertising. Emerging AI technologies can use data “to design, in the moment, the digital material most likely to lead consumers to engage in actions desired by the [advertiser].”228 Take, for example, a Facebook ad, which typically consists of different human-created components, like text, graphics, and hyperlinks.229 Current technologies can already analyze user data to predict which mix of such elements will be most compelling to a particular individual at a given time.230 AIs can go even further, “generating their own content and potentially creating digital business materials without a single component that was directly designed by a human.”231 By incorporating granular personal details about each “data subject,” they can microtarget individuals and more effectively influence them.232 These tools are not just less expensive than human-generated advertising content but may also be more effective.233

2. Disinformation Campaigns

These social media AIs may also be deployed as a means of election interference. During the 2016 election, for instance, Russian actors conducted a highly adaptive disinformation campaign in an effort to shape the political narrative.234 Through the use of AI, they generated millions of pieces of fake news on Twitter, targeting different groups of voters.235 This type of social media activity can have a significant impact on voter behavior236 and has been

229. Id.
230. Id.
231. Id. at 131.
232. Manheim & Kaplan, supra note 8, at 138.
233. Willis, supra note 228, at 131.
235. Id. at 137–44.
used to encourage minority voters to abstain from voting or vote for a third-party candidate.237

“Deepfake” audio, images, and videos could make these disinformation campaigns even more disruptive.238 Deepfakes appear to depict individuals’ real words and actions but are actually fabrications made with facial recognition AIs.239 As deepfakes become more convincing, these manipulations could create particularly dangerous forms of “fake news” and could be used in the days and hours preceding an election to sow confusion and distrust. For example, in 2021, Russia was accused of using deepfakes to trick senior officials in the European Union and gain information on a Russian opposition movement.240 In addition to imitating public officials, deepfakes could also be used to create fake public testimony and influence or disrupt election proceedings.241 For example, states that rely on independent redistricting commissions often allow citizens to testify about how they would like maps to be drawn.242 Fraudulent testimonies have been used in the past and will only become more convincing as these technologies advance.243

3. Election Hacking

AI also amplifies the risk of election hacking. Since the 2000 presidential election, which sowed distrust in paper ballots,244 most states and jurisdictions have embraced electronic voting in some shape or form.245 Electronic voting technologies vary widely by jurisdiction and rely on a wide range of algorithmic and processing tools. These machines can make voting easier and allow votes to be counted more quickly, accurately, and inexpensively.246

However, there is reason to worry that the algorithms used in these technologies could be hacked to change electoral outcomes or steal confidential election information.247 Experts have raised concerns about voting machines’

237. Kamarck, supra note 11.
239. Id.
241. Rudeen, supra note 1, at 276.
242. Id.
243. Id. at 277; Engler, supra note 238; see also Kamarck, supra note 11.
245. Ryan, supra note 84, at 96.
246. Id. at 96–97.
247. Id. at 99–100.
susceptibility to outside manipulation for decades. Not only were these machines “not initially designed with robust security in mind,” but many of these machines’ components are manufactured abroad, creating additional security risks. As one expert explained, “once you’re in the chips, . . . you can hack whole classes of machines, nationwide.” These machines’ manufacturers have vehemently denied these security risks, and some experts have argued that the United States’ decentralized election administration system would make such attacks difficult to conduct on a large scale. But others contend that the coding on these machines is “quite centralized—[o]ne large vendor codes the system for 2,000 jurisdictions across 31 states’ . . . making sabotage a real possibility.” Plus, some machines are installed with remote-access software, which may allow them to be remotely hacked.

AI can also help hackers overcome barriers to widespread election hacking. By using algorithms to analyze vast amounts of data and automate certain processes, hackers can target election systems and overcome cyber defenses more quickly and effectively.

Voter roll maintenance, ballot verification, and redistricting are being transformed by algorithmic technologies. AI’s ability to improve the efficiency, accessibility, and fairness of these processes merits repeating. However, these technologies also present many of the same algorithmic harms identified in other civil rights domains, which are already having a profound effect on voting rights and our democratic processes.

III. OVERCOMING BARRIERS TO PROGRESS AND REFORM

Election administrators must take action to mitigate the risk of algorithmic harm. But, as Commissioner Rebecca Kelly Slaughter of the Federal Trade Commission put it recently, “we must remember that just as [AI] is not magic, neither is any cure to its shortcomings. It will take focused collaboration between policymakers, regulators, technologists, and attorneys to proactively address this technology’s harms while harnessing its promise.”

This Part seeks to highlight for these stakeholders two unique characteristics of election administration that are likely to complicate reform efforts. The first, described in Section III.A, is the political nature of these activities,
which may affect how election administrators use algorithmic decision systems. The second, described in Section III.B, is the decentralized and disuniform nature of election administration in the United States. Finally, in Section III.C, I explain why proposed solutions may inadequately protect voting rights because of these factors and offer several key considerations for future reforms.

A. Politics and the “Good Faith” Assumption

Much of the literature regarding algorithmic harms focus on harms that occur accidentally.\textsuperscript{257} This makes sense. In domains like healthcare, housing, education, employment, financial services, criminal justice, and government administration, AI tools are usually deployed in “good faith,” or in the interest of improving efficiency, cost savings, and accuracy.\textsuperscript{258} Though AIs deployed in service of such goals may still generate inaccurate and discriminatory results, these outcomes are generally rendered inadvertently.\textsuperscript{259} The concern is less that AI users and developers may discriminate intentionally or act with malice and more that their human error and implicit biases will infect algorithmic processes and cause systems to render harmful and biased results.\textsuperscript{260}

The same cannot necessarily be said with regard to election administration. Though many election officials are motivated by the same “good faith” interests, their work cannot be separated from the broader political context.\textsuperscript{261} Each of the election administration activities described in Part II can be and have been used as political weapons.\textsuperscript{262} Voter purges can be ordered for political reasons and intentionally conducted in ways that target or favor certain voting blocs.\textsuperscript{263} Redistricting has similarly been used to “put a thumb on the scale” in favor of a particular political party.\textsuperscript{264} Signature matching, too, has

\textsuperscript{257.} See, e.g., Hoffman & Podgurski, supra note 28; Prince & Schwarcz, supra note 27; Price, supra note 71.

\textsuperscript{258.} See, e.g., Hoffman & Podgurski, supra note 28, at 31 (“Most if not all medical AI algorithm developers are well-intentioned and strive in good faith to improve human health through their work.”).

\textsuperscript{259.} See supra Section I.B.

\textsuperscript{260.} See supra Section I.B.

\textsuperscript{261.} See NAT’L RSCH. COUNCIL, supra note 11, at 49, 63.

\textsuperscript{262.} See, e.g., id.

\textsuperscript{263.} Id.

become increasingly politicized and a heated point of contention in recent elections.265

Further, many election administrators are themselves partisan actors.266 Most secretaries of state, who generally serve as chief state election officials, are elected in partisan contests.267 Thus, they tend to be “ambitious political operators.”268 About half of all local election officials269 and poll workers in many states270 are also openly aligned with a political party.

Even nonpartisan election administrators are subject to outside political pressures. This may come from other public officials, the state legislature, or even their constituents. For example, a nonpartisan election administrator resigned from her position last year after coming under “fierce attacks” from partisan activists and county commissioners for her handling of the 2020 election.271 She is not alone. In several states, party leaders have censured and replaced officials for resisting efforts to delegitimize the 2020 election results.272 And, in recent months, a number of state legislatures have also proposed legislation to “politicize, criminalize, and interfere in election administration.”273

While election administrators may resist these pressures and deploy AIs in good faith, these political forces are likely to infect the incentives surrounding these technologies’ use in some shape or form. Particularly in light of the increased political polarization in the United States, it seems reasonable to conclude that at least some of these systems are—or will be—used or designed not only to improve efficiency but also to advance political ends.


269. Parks, supra note 266.


B. Decentralization and Disuniformity

Election administration in the United States is also highly decentralized and disuniform.\textsuperscript{274} Elections are run by “thousands of state and local systems rather than a single, unified national system.”\textsuperscript{275} States are typically responsible for determining the rules of elections, while local entities administer elections in accordance with those rules.\textsuperscript{276} In some small jurisdictions, a single person may be responsible for administrative activities from registering voters to counting ballots.\textsuperscript{277}

There is also wide variation “in the way voting is run state to state, or even within the same state.”\textsuperscript{278} State and local election officials may be elected or appointed, and either process may occur in a partisan, bipartisan, or nonpartisan manner.\textsuperscript{279} Further, state officials have varying levels of influence over local election officials.\textsuperscript{280} The population size, density, and demographics of the jurisdictions that each system serves can also vary significantly.\textsuperscript{281}

Though this decentralization, at least in theory, enhances election officials’ ability to experiment with new technologies and methodologies, some experts believe it has slowed technological innovation in this domain.\textsuperscript{282} The current structure of election administration makes it difficult to create standardized voting systems.\textsuperscript{283} As a result, there is no central national market for election administration technologies and business solutions.\textsuperscript{284} In this way, our decentralized system may actually stymie the adoption of election AIs.

Decentralization and disuniformity may increase the risk of algorithmic harm in other ways, however. First, it may afford election officials too much deference in how they use these technologies.\textsuperscript{285} As is the case with the signature-matching software discussed in Section II.B, this deference means that

\begin{flushleft}
\textsuperscript{274} See SHANTON, supra note 267, at 1. \\
\textsuperscript{275} Id. \\
\textsuperscript{277} So, supra note 276. \\
\textsuperscript{278} Id. \\
\textsuperscript{279} SHANTON, supra note 267, at ii. \\
\textsuperscript{280} Id. at 15. \\
\textsuperscript{281} Id. at 16–17. \\
\textsuperscript{283} Id. \\
\textsuperscript{284} Id. \\
\textsuperscript{285} Cf. Joshua A. Douglas, Undue Deference to States in the 2020 Election Litigation, 30 WM. & MARY BILL RTS. J. 59, 60 (2021) (arguing that courts have “too readily deferred to state legislatures and election officials on how to administer elections, allowing infringements on the constitutional right to vote without sufficient justification”).
\end{flushleft}
jurisdictions may deploy the same technologies in vastly different ways. In an
effort to achieve even greater efficiency, election officials may even repurpose
an AI or use “faulty input data,” increasing the risk of inaccurate results. This,
when combined with a lack of transparency, may make oversight efforts more
difficult.286 Depending on how it is used, the same AI system may render ac-
curate results in one jurisdiction but lead to gross algorithmic harms in an-
other.287

Deferece to state and local election authorities can also pave the way for
suppressive and discriminatory practices. This has been one of the greatest
disadvantages of our decentralized election system historically.288 The rela-
tively low levels of federal oversight have allowed “anti-democratic pockets of
America . . . to suppress voting, sometimes brutally.”289 The same is true with
algorithmic decisionmaking. Deference in whether and how to deploy these
tools is afforded not only to “good faith” election administrators but also to
those who look to achieve an illicit political end.290

Because the populations that election systems serve can vary so signifi-
cantly, decentralization may also increase the risk of algorithmic harms result-
ing from “contextual bias.”291 Though the training data used to develop
election AIs may accurately reflect the demographics of certain localities, or
even the United States at large, they may be wholly unrepresentative of other
cities or states in which they are deployed. As a result, they may render inac-
curate or biased results in certain settings.

Decentralization can also frustrate federal actions on election administra-
tion.292 Federal laws’ efficacy depends “on how closely states and localities
comply with them,” which is likewise “affected by the duties and structures of
the state and local election systems that implement them.”293 Failure to under-
stand these structures has caused unintended effects from some federal elec-
tion requirements. For example, the Uniformed and Overseas Citizens
Absentee Voting Act (UOCAVA) holds states responsible for some of its re-
quirements, such as transmitting absentee ballots to eligible uniformed ser-
vices and other overseas citizens at least forty-five days before Election Day.294
However, compliance with these requirements is often handled by local offi-
cials.295 As a result, the officials held accountable for UOCAVA violations are

286. See Ryan, supra note 84, at 65.
287. See Price, supra note 71, at 67–68.
288. Stewart, supra note 282.
289. Id.
290. See infra Section III.A.
291. See supra notes 71–73 and accompanying text.
292. See SHANTON, supra note 267, at 18.
293. Id.
295. SHANTON, supra note 267, at 18.
often different from those who more directly failed to comply.\textsuperscript{296} For example, in 2012, the U.S. Department of Justice filed a complaint against the State of Alabama for violating UOCAVA.\textsuperscript{297} In its response, the state explained that local officials were responsible for transmitting absentee ballots and, because these local officials were popularly elected and not subject to removal by state officials, it had limited control over whether or how they complied.\textsuperscript{298}

C. Finding a Path Forward

To date, the United States has been slow to respond to the threats posed by AI.\textsuperscript{299} In general, “[t]here is little oversight of AI development, leaving technology giants free to roam through our data and undermine our rights at will.”\textsuperscript{300}

However, AI experts and legal scholars have proffered a variety of possible solutions to the civil rights issues raised by algorithmic decision systems. Some have put together “algorithmic bias toolkits” to help AI users assess and mitigate such risks.\textsuperscript{301} Others have focused on improving diversity in the technology workforce\textsuperscript{302} and increasing representation in big data.\textsuperscript{303} Some point to intellectual property law as a key area for reform, arguing that this could mitigate the effects of the “algorithm secrecy problem.”\textsuperscript{304} And some have proposed creating a regulatory body, analogous to the Food and Drug Administration, to proactively regulate algorithms before they enter the market.\textsuperscript{305}

Though such reforms could be useful first steps, they are unlikely, standing alone, to adequately address the challenges algorithmic decisionmaking presents in election administration. The efficacy of each of these reforms relies on the “good faith” assumption described above, and thus, they would fail to address the ways algorithmic systems might be designed or used to secure partisan or other advantage.

\textsuperscript{296} Id.
\textsuperscript{297} Id.
\textsuperscript{298} Id.
\textsuperscript{299} Manheim & Kaplan, supra note 8, at 110.
\textsuperscript{300} Id.
\textsuperscript{301} E.g., Ziad Obermeyer et al., CTR. FOR APPLIED A.I. AT CHI. BOOTH, ALGORITHMIC BIAS PLAYBOOK (2021), https://www.chicagobooth.edu/-/media/project/chicago-booth/centers/caai/docs/algorithmic-bias-playbook-june-2021.pdf [perma.cc/B2J5-KCK4]; AI NOW, supra note 37.
\textsuperscript{302} Manheim & Kaplan, supra note 8, at 160.
\textsuperscript{303} See id.; see also Kayte Spector-Bagdady et al., Respecting Autonomy and Enabling Diversity: The Effect of Eligibility and Enrollment on Research Data Demographics, 40 HEALTH AFFS. 1892 (2021).
\textsuperscript{304} Ryan, supra note 84, at 110; see also Raub, supra note 6, at 550.
These proposed reforms are also largely focused on algorithmic harms resulting from faulty programming and design and inadequately address the wide variety of ways that election administrators may use these technologies and their results. Even accurate, responsibly designed AIs can be deployed in ways that yield discriminatory results. As a result, oversight that simply determines which algorithmic systems are fit for use will fail to address the full range of algorithmic harms.

To adequately safeguard voting rights, regulators must address “faulty uses” of AI and both intentional and unintentional “proxy discrimination.” To do so, oversight must be ongoing, and regulators must monitor how these technologies and their results are actually being used to make election decisions. For example, regulators could require election systems that use AI to collect data about subjects’ membership in protected classes. Those data could then be used to assess whether the technologies are yielding discriminatory outcomes, either intentionally or inadvertently.

To be sure, such data might not be sufficient to establish a successful claim under seemingly applicable federal antidiscrimination law. For instance, using AIs that render racially biased results to conduct voter purges might run afoul of section 2 of the Voting Rights Act (VRA), which prohibits electoral practices that result in a “denial or abridgment” of the right to vote based on race or membership in a protected language minority group. And yet, plaintiffs have long struggled to prevail on related section 2 claims. Recent decisions limiting the statute’s application in these contexts, most notably in Brnovich v. Democratic National Committee, suggest the road ahead will be even more difficult. Parsing precisely how plaintiffs bringing AI-based section 2 claims might navigate the new “guideposts” articulated in Brnovich is beyond the scope of this Note. What is clear is that these factors are likely to diminish plaintiffs’ success in all section 2 cases and to pose additional barriers for those challenging algorithmic decisionmaking.

306. See supra Sections I.B.2–3.
308. See id.
312. Katz et al., supra note 310.
313. These guideposts include: (1) “the size of the burden imposed by a challenged voting rule”; (2) “the degree to which a voting rule departs from what was standard practice when [section 2] was amended in 1982”; (3) “[t]he size of any disparities in a rule’s impact on members of different racial or ethnic groups”; (4) “the opportunities provided by a State’s entire system of voting”; and (5) “the strength of the state interests served” by the challenged voting rule. Brnovich, 141 S. Ct. at 2336, 2338–41.
314. Katz et al., supra note 310.
This Note is not intended to provide an exhaustive list of possible solutions to these challenges but rather to provide an initial framework for evaluating proposed reforms. Protecting voting rights and our democratic processes from algorithmic harms requires careful consideration of both the diverse election processes and systems in which these technologies are deployed, as well as the political pressures that plague them. In order to mitigate the risks posed by AI and algorithmic decisionmaking, while also seizing their many benefits, policymakers and advocates must account for the unique characteristics of election administration and voting rights law.

CONCLUSION

AI has entered our election administration, just as it has entered our healthcare institutions, our criminal justice system, and our hiring practices. Civil rights advocates, lawmakers, and legal scholars are right to sound the alarm on algorithmic harms in these and other domains. However, they should not neglect the impact of algorithmic decisionmaking on elections and voting. Each of the election administration activities described in this Note plays a significant role in our elections and democratic processes. They are also being transformed by AI. Election administrators and lawmakers must take thoughtful action to protect U.S. elections and voters from algorithmic harms while retaining the promise of these new tools.