Michigan Law Review

Volume 121 | Issue 3

2022

Algorithmic Elections

Sarah M.L. Bender
University of Michigan Law School

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

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 HARMS ... 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.

 doi:10.36644/mlr.121.3.algorithmic

4. Lack of Transparency 499
II. AUTOMATING ELECTION ADMINISTRATION 501
A. *Maintaining Voter Rolls* 502
B. *Signature Matching* 507
C. *Redistricting* 510
D. *Other Potentially Impactful AI Developments* 512
1. Political Advertising 513
2. Disinformation Campaigns 513
3. Election Hacking 514
III. OVERCOMING BARRIERS TO PROGRESS AND REFORM 515
A. *Politics and the "Good Faith" Assumption* 516
B. *Decentralization and Disuniformity* 518
C. *Finding a Path Forward* 520
CONCLUSION 522

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

1. *See, e.g.*, Jowei Chen & Nicholas O. Stephanopoulos, *The Race-Blind Future of Voting Rights*, 130 YALE L.J. 862, 866 (2021); Emily Rong Zhang, *Bolstering Faith with Facts: Supporting Independent Redistricting Commissions with Redistricting Algorithms*, 109 CALIF. L. REV. 987 (2021); Daniel Oberhaus, *Algorithms Supercharged Gerrymandering. We Should Use Them to Fix It*, VICE: MOTHERBOARD (Oct. 3, 2017, 3:11 PM), https://www.vice.com/en/article/7xkmag/gerrymandering-algorithms [perma.cc/C84F-JC88]; Douglas Rudeen, *The Balk Stops Here: Standards for the Justiciability of Gerrymandering in the Coming Age of Artificial Intelligence*, 56 IDAHO L. REV. 261, 277–78 (2020).

2. Mark Minevich, *7 Ways AI Could Solve All of Our Election Woes: Out with the Polls, In with the AI Models*, FORBES (Nov. 2, 2020, 8:17 AM), https://www.forbes.com/sites/markminevich/2020/11/02/7-ways-ai-could-solve-all-of-our-election-woes-out-with-the-polls-in-with-the-ai-models/?sh=68252669622c [perma.cc/UJR9-6K26].

3. Whitney Clavin, *Algorithms Seek Out Voter Fraud*, CALTECH: NEWS (Nov. 4, 2019), https://www.caltech.edu/about/news/algorithms-seek-out-voter-fraud [perma.cc/XL9K-2DCU].

themselves engage in intentional discrimination.[4] As a result, they have the potential to improve traditional human decisionmaking and to render more objective and less discriminatory results.[5]

Unfortunately, this hope has not borne out in practice. Algorithms have instead proven to be "our opinions embedded in code."[6] 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."[7] 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.[8]

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.[9] Relatively little attention has been given to its use in U.S. elections or its impact on voting rights,[10] 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.

5. *See* James Manyika, Jake Silberg & Brittany Presten, *What Do We Do About the Biases in AI?*, HARV. BUS. REV. (Oct. 25, 2019), https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai [perma.cc/J72V-9LXC].

6. McKenzie Raub, Comment, *Bots, Bias and Big Data: Artificial Intelligence, Algorithmic Bias and Disparate Impact Liability in Hiring Practices*, 71 ARK. L. REV. 529, 533–34 (2018).

7. Rebecca Kelly Slaughter, Janice Kopec & Mohamad Batal, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. (SPECIAL ISSUE) 1, 3 (2021).

8. Karl Manheim & Lyric Kaplan, *Artificial Intelligence: Risks to Privacy and Democracy*, 21 YALE J.L. & TECH. 106, 157 (2019).

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.[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[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.

---

11. Though there is a growing body of literature about AI's use in redistricting, these pieces do not address other forms of algorithmic decisonmaking 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.dellemc.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.org/blogs/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.

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.[13] Similarly, all machine learning involves AI, but not all AI involves machine learning.[14]

Broadly speaking, an algorithm is "a finite series of well-defined, computer-implementable instructions"[15] used to process input data and generate certain outputs.[16] Today, nearly all software programs use some type of algorithm to solve problems and execute tasks.[17] Algorithms can be quite simple, like generating a Fibonacci sequence.[18] 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.[19]

Experts define AI in a variety of ways, but the term generally refers to machines that mimic human intelligence.[20] 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.[21] AI's "ability to extract intelligence from unstructured data" is particularly impactful.[22] Vast amounts of data are generated daily, which, on their face, have little apparent meaning.[23] The goal of AI is to make sense of such data, identifying new patterns and determining how best to act upon them.[24]

---

13. *See, e.g.*, Slaughter, *supra* note 7, at 2 n.1; Eda Kavlakoglu, *AI vs. Machine Learning vs. Deep Learning vs. Neural Networks: What's the Difference?*, IBM: BLOG (May 27, 2020), https://www.ibm.com/cloud/blog/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks [perma.cc/VF6U-HN6F].

14. Slaughter, *supra* note 7, at 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].

16. *The Definitive Glossary of Higher Mathematical Jargon*, *supra* note 15.

17. John R. Allen & Darrell M. West, *The Brookings Glossary of AI and Emerging Technologies*, BROOKINGS (Oct. 11, 2021), https://www.brookings.edu/blog/techtank/2020/07/13/the-brookings-glossary-of-ai-and-emerging-technologies [perma.cc/Z2WV-42MH].

18. *E.g.*, Ali Dasdan, Twelve Simple Algorithms to Compute Fibonacci Numbers (Apr. 16, 2018) (unpublished manuscript), https://doi.org/10.48550/arXiv.1803.07199.

19. Allen & West, *supra* note 17.

20. Kavlakoglu, *supra* note 13.

21. Darrell M. West, *What Is Artificial Intelligence?*, BROOKINGS (Oct. 4, 2018), https://www.brookings.edu/research/what-is-artificial-intelligence [perma.cc/MGF3-TR9S].

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.[25] 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."[26] 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.[27]

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.[28] 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."[29] 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.[30] 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.[31] 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.[32]

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."[33] 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.*

27. Manheim & Kaplan, *supra* note 8, at 114; Anya E.R. Prince & Daniel Schwarcz, *Proxy Discrimination in the Age of Artificial Intelligence and Big Data*, 105 IOWA L. REV. 1257, 1273–75 (2020).

28. Prince & Schwarcz, *supra* note 27, at 1273; Sharona Hoffman & Andy Podgurski, *Artificial Intelligence and Discrimination in Health Care*, 19 YALE J. HEALTH POL'Y, L., & ETHICS, no. 3, 2020, at 1, 8–9.

29. Prince & Schwarcz, *supra* note 27, at 1274.

30. Hoffman & Podgurski, *supra* note 28, at 9.

31. *Id.*

32. *See* Raub, *supra* note 6, at 533–34.

33. Prince & Schwarcz, *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.[34] Human error and bias can infect AIs and algorithms at each of these stages, which can cause them to render inaccurate and discriminatory results.[35] These results may then be used to make high-stakes decisions, like how to allocate a limited supply of COVID-19 vaccines[36] or whether to initiate a child welfare intervention.[37]

"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.[38] Training data can be skewed in a variety of ways, all of which may impair the algorithm's results and produce problematic outcomes.[39]

First, training data may not represent the population they are designed to serve, causing biased and ungeneralizable outcomes.[40] For example, Amazon recently discontinued its use of a recruiting AI after it found the tool was systematically discriminating against female candidates.[41] 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.[42] 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.[43]

---

34. Deborah Won, Note, *The Missing Algorithm: Safeguarding* Brady *Against the Rise of Trade Secrecy in Policing*, 120 MICH. L. REV. 157, 162 (2021).

35. *Id.*

36. Slaughter, *supra* note 7, at 4.

37. AI NOW, ALGORITHMIC ACCOUNTABILITY POLICY TOOLKIT 7 (2018), https://ainowinstitute.org/aap-toolkit.pdf [perma.cc/FPP9-C7VT].

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.

41. Slaughter, *supra* note 7, at 8; Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women*, REUTERS (Oct. 10, 2018, 7:04 PM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-%20scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [perma.cc/6FE3-J59Q]; Nicol Turner Lee, Paul Resnick & Genie Barton, *Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms*, BROOKINGS (May 22, 2019), https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms [perma.cc/VK5X-CKA9].

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.[44] For example, racial and ethnic minorities and low-income individuals often have missing and incorrect information in their medical records.[45] Thus, algorithms trained using medical records may fail to identify significant variables and perform worse for such patients and, generally, across the board.[46]

However, even AIs trained on accurate and fully representative datasets can yield unjust results.[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."[48] Even when data regarding such traits are perfectly accurate, they will reflect the injustices that caused such disparities.[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.[50] Data regarding such traits, however accurate, will reflect these disparities.[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.[52]

Programmers' biases may also infect machine-learning algorithms through "faulty labeling" of training data. Labels instruct algorithms how to distinguish between certain inputs.[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.[54] When one considers the severe lack of diversity in the tech industry—which is "predominantly white, Asian, and male"[55]—it becomes easy to see how programmers' biases can become embedded in these technologies.

---

44. Hoffman & Podgurski, *supra* note 28, at 13.

45. *Id.*

46. *See id.*

47. *Id.* at 18; Deborah Hellman, *Big Data and Compounding Injustice*, 19 J. MORAL PHIL. (forthcoming 2022) (manuscript at 4), https://ssrn.com/abstract=3840175 [perma.cc/GED6-CWXJ].

48. Hellman, *supra* note 47, at 4.

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. Raub, *supra* note 6, at 534.

54. *Id.*; Barocas & Selbst, *supra* note 38, at 679.

55. Raub, *supra* note 6, at 541.

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.[56] 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.[57] 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,"[58] companies continue to sell these technologies and market them as reliable predictors of social outcomes like job performance.[59]

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.[60] A common example is when users place too much stock in the system's results, a phenomenon commonly referred to as "automation bias."[61] Despite their imperfections, AI and algorithmic technologies are shrouded in a "veneer of objectivity."[62] Humans tend to view automated systems as fairer and more reliable than humans.[63] 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.[64] 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.[65] 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.[66]

---

56. Slaughter, *supra* note 7, at 10, 13.

57. *Id.* at 11–12.

58. Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements*, 20 PSYCH. SCI. PUB. INT., no. 1, 2019, at 48.

59. Slaughter, *supra* note 7, at 12.

60. *See* Won, *supra* note 34, at 162.

61. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); *see also* Slaughter, *supra* note 7, at 13.

62. Slaughter, *supra* note 7, at 13.

63. *See* Jeffrey L. Vagle, *Tightening the OODA Loop: Police Militarization, Race, and Algorithmic Surveillance*, 22 MICH. J. RACE & L. 101, 128–30 (2016).

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/10.2514/6.2004-6313 (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.[67] For example, during the COVID-19 pandemic, some hospitals hurriedly repurposed AI systems that were designed and trained for non-pandemic uses and situations.[68] 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.[69] 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.[70]

"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).[71] While an AI trained in one setting may be untinged by problematic bias when deployed in the same and similar contexts,[72] it may render biased results in other contexts if it was not trained to account for such differences.[73]

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.[74] 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.[75] Discriminators can use these kinds of data in facially neutral ways, which nevertheless leads to differing treatment of protected classes.[76] This can occur both intentionally and inadvertently.[77] In either instance, the usefulness of the neutral practice

67. *See* Won, *supra* note 34, at 162.

68. DAVID LESLIE ET AL., DOES "AI" STAND FOR AUGMENTING INEQUALITY IN THE ERA OF COVID-19 HEALTHCARE? 3 (2021), https://doi.org/10.1136/bmj.n304.

69. *Id.*

70. *Id.*

71. W. Nicholson Price II, *Medical AI and Contextual Bias*, 33 HARV. J.L. & TECH. 65, 67–68 (2019) (emphasis omitted).

72. *See id.*

73. *See id.*

74. Prince & Schwarcz, *supra* note 27, at 1267.

75. Raub, *supra* note 6, at 535–36.

76. Prince & Schwarcz, *supra* note 27, at 1267; Slaughter, *supra* note 7, at 20.

77. Raub, *supra* note 6, at 536; Slaughter, *supra* note 7, at 23–24.

"derives, at least in part, from the very fact that it produces a disparate impact"[78] and "often result[s] in disparate treatment of or disparate impact on protected classes for certain economic, social, and civic opportunities."[79]

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.[80] 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.[81] Thus, even if this AI explicitly excludes genetic information from its model to comply with state law,[82] it could still use the Facebook data to proxy discriminate against individuals with certain genetic predispositions.[83]

4. Lack of Transparency

Transparency could help to mitigate concerns regarding algorithms' accuracy and bias and encourage more responsible use of automated technologies.[84] 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.[85]

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.[86] The private companies that develop these tools have claimed that their algorithms are proprietary and must be kept secret to recoup their investments.[87] 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.

80. Prince & Schwarcz, *supra* note 27, at 1261–62.

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].

83. Prince & Schwarcz, *supra* note 27, at 1261–62.

84. Meghan J. Ryan, *Secret Algorithms, IP Rights, and the Public Interest*, 21 NEV. L.J. 61, 65 (2020).

85. *See id.* at 64.

86. Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1346–48, 1393–94 (2018); Won, *supra* note 34, at 165.

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."[88]

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.[89] As a result, AI programmers, users, and AIs themselves are often unable to explain how or why these "black box" algorithms reached certain conclusions.[90] 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."[91]

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.[92] For example, the "requirement of purpose" doctrine "reads an intentionality requirement into the Equal Protection [C]lause," meaning actions that cause discriminatory results are only unconstitutional if the discrimination is intended.[93] 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.[94] 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].

88. Ryan, *supra* note 84, at 65; *see also* Rebecca Wexler, *Convicted by Code*, SLATE (Oct. 6, 2015, 12:28 PM), https://slate.com/technology/2015/10/defendants-should-be-able-to-inspect-software-code-used-in-forensics.html [perma.cc/MHL9-E233].

89. *See* Manheim & Kaplan, *supra* note 8, at 153–54.

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)).

94. Prince & Schwarcz, *supra* note 27, at 1274; *see also* Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 906 (2018).

efficiency and cost savings.[95] As a result, algorithmic decisionmaking may be beyond the reach of equal protection doctrine regardless of how biased it is.[96]

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,[97] assess the risk of recidivism to determine sentencing,[98] and identify and find suspects using photos and videos.[99] Advocates have also sounded the alarm on algorithmic bias in consumer lending,[100] housing,[101] education,[102] employment,[103] healthcare,[104] and the allocation of government services and benefits.[105]

---

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-inequity-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.

97. ANDREW GUTHRIE FERGUSON, THE RISE OF BIG DATA POLICING 73 (2017).

98. *See, e.g.,* Julia Dressel & Hany Farid, *The Accuracy, Fairness, and Limits of Predicting Recidivism*, SCI. ADVANCES, Jan. 17, 2018, at 1.

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

100. *See, e.g.*, Aaron Klein, *Reducing Bias in AI-Based Financial Services*, BROOKINGS (July 10, 2020), https://www.brookings.edu/research/reducing-bias-in-ai-based-financial-services [perma.cc/EF57-ANXW].

101. *See, e.g.*, Lauren Sarkesian & Spandana Singh, *HUD's New Rule Paves the Way for Rampant Algorithmic Discrimination in Housing Decisions*, NEW AM. (Oct. 1, 2020), https://www.newamerica.org/oti/blog/huds-new-rule-paves-the-way-for-rampant-algorithmic-discrimination-in-housing-decisions [perma.cc/F8YU-3R3H].

102. *See, e.g.*, Andre M. Perry & Nicol Turner Lee, *AI Is Coming to Schools, and If We're Not Careful, So Will Its Biases*, BROOKINGS (Sept. 26, 2019), https://www.brookings.edu/blog/the-avenue/2019/09/26/ai-is-coming-to-schools-and-if-were-not-careful-so-will-its-biases [perma.cc/R5QX-5954].

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.[106] 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.[107] 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[108] 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*.[109] 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.[110] 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."[111] After a voter registry is created, states must keep ineligible voters off the registration lists and add newly registered voters to them.[112]

The practice of removing voters from these lists is commonly referred to as "voter purging."[113] Voters can lose their eligibility for a variety of reasons, including changes in residence, felony convictions, mental incapacity findings, death, or inactivity.[114] 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.

109. 139 S. Ct. 2484 (2019).

110. 52 U.S.C. § 21083(a)(1)(A).

111. NAT'L RSCH. 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.[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.[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.[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."[118] Voter purges can also be used to manipulate election outcomes[119] and to discriminate against poor and minority voters.[120] Though the National Voter Registration Act (NVRA)[121] set federal standards for voter purges in 1993, states continue to conduct illegal purges and adopt policies that violate the NVRA.[122]

Because voter registration lists generally contain millions of entries, purges must be at least partially automated.[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.[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

115. Gregory A. Huber, Marc Meredith, Michael Morse & Katie Steele, *The Racial Burden of Voter List Maintenance Errors: Evidence from Wisconsin's Supplemental Movers Poll Books*, SCI. ADVANCES, Feb. 17, 2021, at 1.

116. JONATHAN BRATER, BRENNAN CTR. FOR JUST. AT N.Y.U. SCH. OF L., VOTER PURGES: THE RISKS IN 2018, at 1 (2018), https://www.brennancenter.org/sites/default/files/2019-08/Report_Voter_Purges_The_Risks_in_2018.pdf [perma.cc/Y9JV-5NUR].

117. *Id.*

118. Huber et al., *supra* note 115, at 1.

119. NAT'L RSCH. COUNCIL, *supra* note 11, at 49.

120. *See* Sean Holstege, *Do Voter Purges Discriminate Against the Poor and Minorities?*, NBC NEWS (Aug. 24, 2016, 12:07 PM), https://www.nbcnews.com/news/us-news/do-voter-purges-discriminate-against-poor%20minorities-n636586 [perma.cc/AS5W-6639]. Relatedly, purge rates have increased most in jurisdictions previously subject to federal preclearance requirements under the Voting Rights Act. JONATHAN BRATER, KEVIN MORRIS, MYRNA PÉREZ & CHRISTOPHER DELUZIO, BRENNAN CTR. FOR JUST. AT N.Y.U. SCH. OF L., PURGES: A GROWING THREAT TO THE RIGHT TO VOTE 3 (2018), https://www.brennancenter.org/media/235/download [perma.cc/SB6U-B8TK].

121. 52 U.S.C. §§ 20501–20511.

122. BRATER ET AL., *supra* note 120, at 1–2.

123. NAT'L RSCH. COUNCIL, *supra* note 11, at 46.

124. *Id.*

obtaining a driver's license."[125] The same name may also refer to many different people, or names may be misspelled.[126] Name-matching algorithms are widely used to overcome these challenges.[127]

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.[128] As a result, roughly 2.75 million Americans were on more than one state's voter rolls as of 2012.[129]

Interstate cross-checking became feasible after states began to centralize, standardize, and digitize their voter rolls in 2002 as part of HAVA.[130] 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.[131] Crosscheck worked by comparing states' voter files and sending participating states a list of voter registrations that matched those of another state.[132] Though states could use this information however they wished, Crosscheck provided guidelines for purging these voters' records.[133]

Another interstate cross-checking initiative has since taken hold. A nonprofit organization called the Electronic Registration Information Center (ERIC) uses algorithm processes[134] to assist thirty states and the District of Columbia in identifying unregistered individuals and maintaining accurate voter registries.[135] ERIC generates two types of lists for member states: (1) lists

125. *Id.* at 47.

126. *Id.*

127. *Id.* at 48.

128. Alexander Siegal, *Voter Fraud's False Advertisers: Partisanship and Preventing Another Kansas Interstate Voter Registration Crosscheck Program*, 1 N.Y.U. AM. PUB. POL'Y REV. 25, 25 (2021).

129. *Id.*

130. *Id.* at 26.

131. *Id.*

132. *Id.*; Christopher Ingraham, *This Anti-Voter-Fraud Program Gets It Wrong over 99 Percent of the Time. The GOP Wants to Take It Nationwide.*, WASH. POST (July 20, 2017), https://www.washingtonpost.com/news/wonk/wp/2017/07/20/this-anti-voter-fraud-program-gets-it-wrong-over-99-of-the-time-the-gop-wants-to-take-it-nationwide [perma.cc/2W3G-UT74].

133. Ingraham, *supra* note 132.

134. *See* Huber et al., *supra* note 115, at 3 (describing ERIC's system as an "algorithmic process"); ELEC. REGISTRATION INFO. CTR., ERIC: TECHNOLOGY AND SECURITY OVERVIEW 2–3 (2021), https://ericstates.org/wp-content/uploads/2022/02/ERIC_Tech_and_Security_Brief_v5.0.pdf [perma.cc/YLF7-5P6Y] (describing ERIC's use of record linkage algorithms).

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.[136] 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.[137]

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.[138] Specifically, these tools rendered more "mismatches" for Asian names.[139]

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[140] after researchers found that the tool was overrun with security flaws and false positives.[141] 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.[142] These voter records were purged, jeopardizing these eligible voters' ability to cast a ballot.[143]

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.[144] However, because its lists are also used in states' voter purges,[145] it has the

136. Huber et al., *supra* note 115, at 2.

137. *Id.* at 1.

138. Alexandros Karakasidis & Evaggelia Pitoura, *Identifying Bias in Name Matching Tasks*, *in* ADVANCES IN DATABASE TECHNOLOGY—EDBT 2019 (Melanie Herschel et al. eds., 2019), https://openproceedings.org/2019/conf/edbt/EDBT19_paper_213.pdf [perma.cc/9WXT-HA64].

139. *Id.*

140. *ACLU of Kansas Settlement Puts "Crosscheck" Out of Commission for Foreseeable Future*, ACLU OF KANSAS (Dec. 10, 2019), https://www.aclukansas.org/en/press-releases/aclu-kansas-settlement-puts-crosscheck-out-commission-foreseeable-future-program [perma.cc/H8DM-YSFS].

141. *Moore v. Schwab (Previously Moore v. Kobach)*, ACLU OF KANSAS (June 19, 2018), https://www.aclukansas.org/en/cases/moore-v-schwab-previously-moore-v-kobach [perma.cc/LA8T-VW7A].

142. Sharad Goel et al., *One Person, One Vote: Estimating the Prevalence of Double Voting in U.S. Presidential Elections*, 114 AMER. POL. SCI. REV. 456, 466 (2020).

143. *See id.*

144. Huber et al., *supra* note 115, at 2; *see also* Steve Lohr, *Another Use for A.I.: Finding Millions of Unregistered Voters*, N.Y. TIMES (Nov. 5, 2018), https://www.nytimes.com/2018/11/05/technology/unregistered-voter-rolls.html [perma.cc/5PEH-WFGU].

145. Huber et al., *supra* note 115, at 1.

same capacity for voter disenfranchisement.[146] ERIC member states contact voters who are flagged as having moved or no longer being eligible to vote.[147] 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."[148] 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.[149] 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.[150]

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.[151] 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.[152]

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.[153] 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.[154] 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.[155] Using SAVE in this way risked disenfranchising eligible voters, particularly those who had recently become naturalized citizens.[156] This practice was challenged, and, in 2014, the

146. *See id.* at 2.

147. *Id.*

148. 138 S. Ct. 1833, 1856 (2018) (Breyer, J., dissenting).

149. *Id.*

150. *Id.*

151. Huber et al., *supra* note 115, at 2–3.

152. *Id.* at 7–8.

153. Fatma Marouf, *The Hunt for Noncitizen Voters*, 65 STAN. L. REV. ONLINE 66–67 (2012); Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633, 683–84 (2017).

154. Marouf, *supra* note 153, at 67; Hu, *supra* note 153, at 683–84.

155. Marouf, *supra* note 153, at 67–68.

156. *Id.* at 68; *see also* Hu, *supra* note 153, at 683–84.

Eleventh Circuit found it to violate the NVRA for this reason.[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.[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.[159] Before the vast majority of these votes were counted, they underwent a signature-matching test.[160] As of 2020, thirty-three states required validation of voters' signatures on mail-in ballots.[161] In the 2016 elections, signature discrepancies were the most common reason for rejecting mail-in ballots,[162] and, over the course of the 2016 and 2018 elections, more than 750,000 absentee ballots were voided during the signature-matching process.[163]

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

157. Arcia v. Fla. Sec'y of State, 772 F.3d 1335, 1348 (11th Cir. 2014).

158. *See* BRATER ET AL., *supra* note 120.

159. Sabri Ben-Achour, *Robots Will Be Verifying Some of Our Ballots. Can We Trust Them?*, MARKETPLACE (Oct. 30, 2020), https://www.marketplace.org/shows/marketplace-tech/vote-by-mail-ballots-mismatched-signatures-verification-software-disenfranchisement [perma.cc/92M2-338L].

160. Kyle Wiggers, *Automatic Signature Verification Software Threatens to Disenfranchise U.S. Voters*, VENTUREBEAT (Oct. 25, 2020, 10:25 AM), https://venturebeat.com/2020/10/25/automatic-signature-verification-software-threatens-to-disenfranchise-u-s-voters [perma.cc/E8J4-UEHK].

161. *Id.*

162. Ben-Achour, *supra* note 159.

163. Wiggers, *supra* note 160.

164. David A. Graham, *Signed, Sealed, Delivered—Then Discarded*, ATLANTIC (Oct. 21, 2020, 5:47 PM), https://www.theatlantic.com/ideas/archive/2020/10/signature-matching-is-the-phrenology-of-elections/616790 [perma.cc/7TVF-GC7W].

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

166. Paresh Dave & Andy Sullivan, *Factbox: U.S. Counties Using Automated Signature Verification Software*, REUTERS (Sept. 24, 2020, 7:07 AM), https://www.reuters.com/article/us-usa-election-ballot-signatures-softwa/factbox-u-s-counties-using-automated-signature-verification-software-idUSKCN26F1U4 [perma.cc/SSH8-Y5YP].

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.

170. *Parascript Solutions for Election Systems*, PARASCRIPT, https://www.parascript.com/solutions-by-industry/government/vote-by-mail-signature-verification [perma.cc/NY4E-Z33V]; *see also* Ben-Achour, *supra* note 159; ARJON ET AL., *supra* note 11, at 1.

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.[179] Other counties require staff to verify each ballot, regardless of the AI's results.[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.[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.[182] For example, existing signature-matching software programs are often trained only on English handwriting.[183] As a result, voters who do not write in English may be at a greater risk of having their ballot rejected.[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.[185] Further, studies have repeatedly found that young voters,[186] elderly voters,[187] voters with disabilities,[188] voters of color,[189] and first-time mail-in voters[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."[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

179. ARJON ET AL., *supra* note 11, at 23.

180. *Id.*

181. Wiggers, *supra* note 160.

182. Ben-Achour, *supra* note 159.

183. Wiggers, *supra* note 160.

184. *Id.*

185. Maya Lau & Laura J. Nelson, *'Ripe for Error': Ballot Signature Verification Is Flawed—And a Big Factor in the Election*, L.A. TIMES (Oct. 28, 2020, 5:27 AM), https://www.latimes.com/california/story/2020-10-28/2020-election-voter-signature-verification [perma.cc/2YJF-268M].

186. *See id.*; Graham, *supra* note 164.

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].

188. Carpenter, *supra* note 187; Lau & Nelson, *supra* note 185; Graham, *supra* note 164.

189. *See* Lau & Nelson, *supra* note 185; Wiggers, *supra* note 160.

190. Lau & Nelson, *supra* note 185; Graham, *supra* note 164.

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.

193. ARJON ET AL., *supra* note 11, at 30.

194. *See* Ben-Achour, *supra* note 159.

195. ARJON ET AL., *supra* note 11, at 30.

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.

202. Rucho v. Common Cause, 139 S. Ct. 2484, 2512–13 (2019) (Kagan, J., dissenting) (providing a brief history of partisan gerrymandering in the United States).

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.[204]

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

This decision has paved the way for even more sophisticated technologies, like AI, to infect redistricting processes.[209] Though much attention has been given to AI's potential to make redistricting less partisan,[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."[211] Machine-learning technologies outperform current redistricting tools, which still struggle to capture nonlinear and context-dependent voting behavior.[212] In contrast, AI tools can identify new patterns and predictive variables,[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.[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.[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.[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

204. Louise Matsakis, *Big Data Supercharged Gerrymandering. It Could Help Stop It Too*, WIRED (June 28, 2019, 2:01 PM), https://www.wired.com/story/big-data-supercharged-gerrymandering-supreme-court [perma.cc/JE96-DKZT]; *Rucho*, 139 S. Ct. at 2513 (Kagan, J., dissenting).

205. Political Science Professors Brief, *supra* note 203, at 23–25.

206. Rudeen, *supra* note 1, at 262.

207. *Rucho*, 139 S. Ct. at 2506–07.

208. Rudeen, *supra* note 1, at 273.

209. *Id.*

210. *E.g.*, Oberhaus, *supra* note 1; Chen & Stephanopoulos, *supra* note 1, at 866.

211. Rudeen, *supra* note 1, at 261.

212. *See* Political Science Professors Brief, *supra* note 203, at 20–21.

213. *Id.* at 25–28.

214. Rudeen, *supra* note 1, at 272; *see also* Political Science Professors Brief, *supra* note 203, at 25–28.

215. Political Science Professors Brief, *supra* note 203, at 28–30.

216. *See id.*

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."[217] Though federal law more clearly prohibits racial gerrymandering, guidance on the issue remains murky.[218] Further, partisanship and race are closely connected in many parts of the country,[219] making racial and partisan gerrymanders "increasingly difficult to tease apart."[220] 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,[221] AI amplifies the risk in several ways. First, AIs may proxy discriminate *accidentally*.[222] 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.[223]

AI may also make it harder to rectify instances of proxy discrimination.[224] 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.[225] 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.[226] This can increase such tools' "appearance of impartiality" and thus also the risk of automation bias.[227]

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

217. Rudeen, *supra* note 1, at 275.

218. *Id.* at 273.

219. Kristen Clarke & Jon Greenbaum, *Gerrymandering Symposium: The Racial Implications of Yesterday's Partisan Gerrymandering Decision*, SCOTUSBLOG (June 28, 2019, 2:01 PM), https://www.scotusblog.com/2019/06/gerrymandering-symposium-the-racial-implications-of-todays-partisan-gerrymandering-decision [perma.cc/G3WJ-LQSL].

220. Rudeen, *supra* note 1, at 262.

221. Slaughter, *supra* note 7, at 23 ("[T]he use of facially neutral factors that generate discriminatory results is something that society and civil rights laws have been grappling with for decades.").

222. *Id.*; Prince & Schwarcz, *supra* note 27, at 1262–64, 1270–76.

223. *See* Slaughter, *supra* note 7, at 23; Prince & Schwarcz, *supra* note 27, at 1262–64, 1270–76.

224. *See* Slaughter, *supra* note 7, at 23.

225. *Id.* at 22–23.

226. *Id.* at 23.

227. *Id.* at 22.

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 behavior[236] and has been

228. Lauren E. Willis, *Deception by Design*, 34 HARV. J.L. & TECH. 115, 130 (2020).

229. *Id.*

230. *Id.*

231. *Id.* at 131.

232. Manheim & Kaplan, *supra* note 8, at 138.

233. Willis, *supra* note 228, at 131.

234. Manheim & Kaplan, *supra* note 8, at 134–37.

235. *Id.* at 137–44.

236. *See* Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335 (2014) (describing a 2010 experiment on "digital gerrymandering" that found that users were more likely to turn out—in electorally significant numbers—when shown news that their friends had voted); Paul Lewis, '*Fiction Is Outperforming Reality*': *How YouTube's Algorithm Distorts Truth*, GUARDIAN (Feb. 2, 2018, 7:00 AM), https://www.theguardian.com/technology/2018/feb/02/how-youtubes-algorithm-distorts-truth [perma.cc/XXY3-A6GP]; Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, NEW REPUBLIC (June 1, 2014), https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering [perma.cc/3QPB-N3N2].

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.

238. Alex Engler, *Fighting Deepfakes When Detection Fails*, BROOKINGS (Nov. 14, 2019), https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails [perma.cc/GTE5-USXT].

239. *Id.*

240. Tony Ho Tran, *Russia Accused of Using Deepfakes to Imitate Political Rivals*, FUTURISM: THE BYTE (Apr. 25, 2021), https://futurism.com/the-byte/russia-accused-using-deepfakes-imitate-political-rivals [perma.cc/ZA3K-YXW5].

241. Rudeen, *supra* note 1, at 276.

242. *Id.*

243. *Id.* at 277; Engler, *supra* note 238; *see also* Kamarck, *supra* note 11.

244. *See* Daniel P. Tokaji, *The Paperless Chase: Electronic Voting and Democratic Values*, 73 FORDHAM L. REV. 1711, 1724–34 (2005).

245. Ryan, *supra* note 84, at 96.

246. *Id.* at 96–97.

247. *Id.* at 99–100.

susceptibility to outside manipulation for decades.[248] 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.[249] As one expert explained, "[o]nce you're in the chips, . . . you can hack whole classes of machines, nationwide."[250] 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.[251] 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."[252] Plus, some machines are installed with remote-access software, which may allow them to be remotely hacked.[253]

AI can also help hackers overcome barriers to widespread election hacking.[254] 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.[255]

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."[256]

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,

248. *Id.* at 99; *see also* Manheim & Kaplan, *supra* note 8, at 136.

249. Ryan, *supra* note 84, at 99, 102.

250. *Id.* at 102.

251. *Id.* at 101.

252. *Id.* at 102.

253. *Id.*

254. Manheim & Kaplan, *supra* note 8, at 136.

255. *Id.*

256. Slaughter, *supra* note 7, at 6.

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.[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.[258] Though AIs deployed in service of such goals may still generate inaccurate and discriminatory results, these outcomes are generally rendered inadvertently.[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.[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.[261] Each of the election administration activities described in Part II can be and have been used as political weapons.[262] Voter purges can be ordered for political reasons and intentionally conducted in ways that target or favor certain voting blocs.[263] Redistricting has similarly been used to "put a thumb on the scale" in favor of a particular political party.[264] Signature matching, too, has

257. *See, e.g.*, Hoffman & Podgurski, *supra* note 28; Prince & Schwarcz, *supra* note 27; Price, *supra* note 71.

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.").

259. *See supra* Section I.B.

260. *See supra* Section I.B.

261. *See* NAT'L RSCH. COUNCIL, *supra* note 11, at 49, 63.

262. *See, e.g.*, *id.*

263. *Id.*

264. Julia Kirschenbaum & Michael Li, *Gerrymandering Explained*, BRENNAN CTR. FOR JUST. (Aug. 12, 2021), https://www.brennancenter.org/our-work/research-reports/gerrymandering-explained [perma.cc/2R47-KW7S].

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 officials[269] and poll workers in many states[270] 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.

---

265. *See, e.g.*, Salvador Rizzo, *Trump's Latest Falsehood: Democrats Are Trying to End Signature Verification for Ballots*, WASH. POST (Aug. 11, 2020, 3:00 AM), https://www.washingtonpost.com/politics/2020/08/11/trumps-latest-falsehood-democrats-are-trying-end-signature-verification-ballots [perma.cc/D2G3-JZSW].

266. Miles Parks, *Partisan Election Officials Are 'Inherently Unfair' but Probably Here to Stay*, NPR (Nov. 29, 2018, 5:00 AM), https://www.npr.org/2018/11/29/671524134/partisan-election-officials-are-inherently-unfair-but-probably-here-to-stay [perma.cc/BN7L-TZAJ].

267. KAREN L. SHANTON, CONG. RSCH. SERV., R45549, THE STATE AND LOCAL ROLE IN ELECTION ADMINISTRATION 12–13 (2019).

268. Siegal, *supra* note 128, at 26.

269. Parks, *supra* note 266.

270. *See* U.S. ELECTION ASSISTANCE COMM'N, STATE-BY-STATE COMPENDIUM: ELECTION WORKER LAWS & STATUTES (4th ed. 2020), https://www.eac.gov/sites/default/files/electionofficials/pollworkers/Compendium_2020.pdf [perma.cc/H7SY-HPCQ].

271. Michele Carew, *Partisan Attacks Drove Me Out of My Job as a Texas Elections Official*, WASH. POST (Nov. 1, 2021, 9:00 AM), https://www.washingtonpost.com/opinions/2021/11/01/partisan-attacks-drove-me-out-my-job-texas-elections-official [perma.cc/MXB3-PZWZ].

272. BRENNAN CTR. FOR JUST. AT N.Y.U. SCH. OF L., ELECTION OFFICIALS UNDER ATTACK (2021), https://www.brennancenter.org/sites/default/files/2021-06/BCJ-130_Election%20Officials_fact%20sheet.pdf [perma.cc/Q3FD-RV9Y].

273. STATES UNITED DEMOCRACY CTR., PROTECT DEMOCRACY & LAW FORWARD, MEMORANDUM: DEMOCRACY CRISIS REPORT UPDATE (2021), https://statesuniteddemocracy.org/wp-content/uploads/2021/06/Democracy-Crisis-Part-II_June-10_Final_v7.pdf [perma.cc/98RC-R4SP].

B. *Decentralization and Disuniformity*

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

There is also wide variation "in the way voting is run state to state, or even within the same state."[278] State and local election officials may be elected or appointed, and either process may occur in a partisan, bipartisan, or nonpartisan manner.[279] Further, state officials have varying levels of influence over local election officials.[280] The population size, density, and demographics of the jurisdictions that each system serves can also vary significantly.[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.[282] The current structure of election administration makes it difficult to create standardized voting systems.[283] As a result, there is no central national market for election administration technologies and business solutions.[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.[285] As is the case with the signature-matching software discussed in Section II.B, this deference means that

---

274. *See* SHANTON, *supra* note 267, at 1.

275. *Id.*

276. *Id.* at 3, 7; Linda So, *Factbox: Who Runs America's Elections?*, REUTERS (June 11, 2021, 6:34 PM), https://www.reuters.com/world/us/who-runs-americas-elections-2021-06-11 [perma.cc/SE3L-YFTJ].

277. So, *supra* note 276.

278. *Id.*

279. SHANTON, *supra* note 267, at ii.

280. *Id.* at 15.

281. *Id.* at 16–17.

282. *See, e.g.*, *Administering Elections in a Hyper-Partisan Era*, MIT POL. SCI. (Oct. 21, 2021), https://polisci.mit.edu/news/2021/administering-elections-hyper-partisan-era [perma.cc/3LHM-ZXY2].

283. *Id.*

284. *Id.*

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").

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 accurate results in one jurisdiction but lead to gross algorithmic harms in another.[287]

Deference 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 relatively 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 significantly, decentralization may also increase the risk of algorithmic harms resulting 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 inaccurate or biased results in certain settings.

Decentralization can also frustrate federal actions on election administration.[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 understand these structures has caused unintended effects from some federal election requirements. For example, the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) holds states responsible for some of its requirements, such as transmitting absentee ballots to eligible uniformed services and other overseas citizens at least forty-five days before Election Day.[294] However, compliance with these requirements is often handled by *local* officials.[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.*
294. 52 U.S.C. § 20302(a)(8).
295. SHANTON, *supra* note 267, at 18.

often different from those who more directly failed to comply.[296] For example, in 2012, the U.S. Department of Justice filed a complaint against the State of Alabama for violating UOCAVA.[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.[298]

C. *Finding a Path Forward*

To date, the United States has been slow to respond to the threats posed by AI.[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."[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.[301] Others have focused on improving diversity in the technology workforce[302] and increasing representation in big data.[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."[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.[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.

---

296. *Id.*

297. *Id.*

298. *Id.*

299. Manheim & Kaplan, *supra* note 8, at 110.

300. *Id.*

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.

302. Manheim & Kaplan, *supra* note 8, at 160.

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).

304. Ryan, *supra* note 84, at 110; *see also* Raub, *supra* note 6, at 550.

305. *See, e.g.*, Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 90 (2017).

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.[306] 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.[307] Those data could then be used to assess whether the technologies are yielding discriminatory outcomes, either intentionally or inadvertently.[308]

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.[309] And yet, plaintiffs have long struggled to prevail on related section 2 claims.[310] Recent decisions limiting the statute's application in these contexts, most notably in *Brnovich v. Democratic National Committee*,[311] suggest the road ahead will be even more difficult.[312] Parsing precisely how plaintiffs bringing AI-based section 2 claims might navigate the new "guideposts"[313] 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[314] and to pose additional barriers for those challenging algorithmic decisionmaking.

---

306. *See supra* Sections I.B.2–3.

307. *See* Prince & Schwarcz, *supra* note 27, at 1311–13.

308. *See id.*

309. 52 U.S.C. § 10301; *see also Section 2 of the Voting Rights Act*, U.S. DEP'T OF JUST. (Nov. 8, 2021), https://www.justice.gov/crt/section-2-voting-rights-act [perma.cc/D8HU-CZ5M].

310. Ellen D. Katz et al., *The Evolution of Section 2: Numbers and Trends*, UNIV. MICH. L. SCH. VOTING RTS. INITIATIVE (2022), https://voting.law.umich.edu/findings [perma.cc/HYP3-8QPS].

311. 141 S. Ct. 2321 (2021).

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.