Racist Robots? The Future of Title VII Disparate Impact Cases in the World of Artificial Intelligence

Jenna Jonjua*

I. INTRODUCTION

From robotic vacuums[1] to gourmet meal cooking machines,[2] the automated lifestyle that Americans first saw on *The Jetsons* in the 1960s is not far from reality today.[3] In early 2019, a survey from National Public Radio and Edison Research found that smart speaker (Amazon Echo, Google Home, Apple HomePod, etc.) ownership increased to 53 million, meaning that 21 percent of U.S. adults owned a smart speaker around the beginning of 2019.[4] Market and consumer data firm Statista predicts that "smart home" technology will have a household penetration of 40.1 percent in 2021, and that the industry will have an annual growth rate of 12.82 percent until 2024.[5] Artificial intelligence

* J.D. 2021, University of Minnesota Law School. I would like to extend my deepest gratitude to my parents and partner for their unconditional support and patience, to my family for teaching me that learning is a lifelong pursuit, and to the faculty and student staff that helped in editing this piece. This is ours.

1. Raghav Bharadwaj, *Artificial Intelligence in Home Robots - Current and Future Use-Cases*, EMERJ (Nov. 22, 2019), https://emerj.com/ai-sector-overviews/artificial-intelligence-home-robots-current-future-use-cases/.

2. SUVIE, https://www.suvie.com/ (last visited Jan. 20, 2019).

3. Nina Zipkin, *8 Far-Out 'Jetson's' Contraptions That Actually Exist Today*, ENTREPRENEUR (Apr. 17, 2015) https://www.entrepreneur.com/article/245192; *but see* Jonathan Vanian, Rosie the Robot Won't be Cleaning Your House Anytime Soon, FORTUNE (June 24, 2016, 7:30 AM), https://fortune.com/2016/06/24/rosie-the-robot-data-sheet/.

4. Nat'l Pub. Radio & Edison Rsch., *The Smart Audio Report*, Nat'l Pub. Media (last visited Dec. 2, 2019), https://www.nationalpublicmedia.com/wp-content/uploads/2019/01/Smart-Audio-Report-Winter-2018.pdf [https://web.archive.org/web/20191202215230/https://www.nationalpublicmedia.com/wp-content/uploads/2019/01/Smart-Audio-Report-Winter-2018.pdf].

5. *Smart Home*, STATISTA, https://www.statista.com/outlook/279/109/smart-home/united-states (last visited June 26, 2021) [https://web.archive.org/web/20210626025922/https://www.statista.com/outlook/dmo/smart-home/united-states].

(AI), the basis of all of these technologies, is rapidly transforming nearly every facet of life. As in *The Jetsons*, the transformation is taking place far beyond the confines of the home. Employers are using AI-based technology to target talent in the recruiting process, screen applicants in the hiring phase, and track employee engagement to help human resources (HR) professionals predict when employees will leave.[6]

It is no wonder that the proliferation of AI-based technology has far outpaced the laws regulating the creation and use of such technology. Despite former President Donald Trump's executive order on AI, the United States has no federal laws specifically aimed at regulating the creation and use of artificial intelligence.[7] This gives rise to several issues, particularly in the area of employment law. While most AI technologies marketed to employers tout themselves as unbiased means of finding talent, AI algorithms are not immune to bias. Title VII claims under current law are decided based on a burden-shifting framework that, after a *prima facie* case is pled by the plaintiff, requires an employer to point to a legitimate, "non-discriminatory" reason for its action at issue. Understanding that AI is not bias-free, it is unclear how existing law would address whether an algorithm is truly non-discriminatory, whether dependence on such an algorithm (biased or not) would be a defense for employers, or how liability should be assigned in such a scenario. Further, this opacity regarding how algorithms work exacerbates existing power imbalances and information inequality between employers and employees. This Article proposes, in addition to other reforms, the U.S. will need to take a clearer, more cohesive approach to regulating data privacy and managing data processing in order to deal with the legal ambiguities caused by the proliferation of AI-based technology in the employment area and beyond. The European Union's General Data Protection Regulation (GDPR) created key rights and expectations surrounding data regulation that would make application of existing employment laws easier with the introduction of AI into decision making.[8] This Article then

6. Dom Nicastro, *7 Ways Artificial Intelligence in Reinventing Human Resources*, CMS WIRE (May 18, 2018), https://www.cmswire.com/digital-workplace/7-ways-artificial-intelligence-is-reinventing-human-resources/.

7. *See AI Policy – United States*, FUTURE OF LIFE INST., https://futureoflife.org/ai-policy-united-states/ (last visited Jan. 24, 2020).

8. Council Regulation 2016/679 of Apr. 27, 2016, On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data

reviews proposed solutions to the legal ambiguities of AI in human resources, and explains why data-focused reforms are foundational in order to adapt existing legal frameworks to the new age of big data economy.

This Article aims to explore the applicability of the current *McDonnell-Douglas* burden-shifting framework for employment discrimination claims in evaluating employer decisions made using AI-based technology. Part I will provide insight into what artificial intelligence is, how employment discrimination claims are currently evaluated, and the GDPR's framework for data protection. Part II explores the process of proving disparate impact claims and how AI will change the effectiveness of that framework in light of the data-driven problems that result from the use of AI in employment decisions. Part III will show how the GDPR is an example of a data privacy-focused framework for addressing the proliferation of big data and, consequently, AI. Ultimately, Part IV will review some of the important short-term solutions for harnessing the potential of AI, while mitigating against some of the risks it poses. It also shows how the GDPR's standards can inspire more robust, fair development and use of AI technology in the employment decision-making process.

II. BACKGROUND

A. WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial Intelligence is a form of technology where machines have the ability to "learn" from data analysis and task performance, thus allowing the machines to adapt their "behavior" to improve performance over time.[9] There are two primary components of AI: 1) algorithms, or programmed functions that process data, and 2) the data inputs that those algorithms review.[10] The algorithms give the AI technologies the guidance they need to process immense sets of data.[11] It has been suggested that the use of algorithms to remove race, gender, and

---

Protection Regulation), 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

9. PRACTICAL LAW LABOR & EMPLOYMENT, ARTIFICIAL INTELLIGENCE (AI) IN THE WORKPLACE, Westlaw (database updated June 2021), Westlaw Practical Law Practice Note w-018-7465.

10. *Id.*

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

national origin from the original evaluation process can reduce unconscious bias and lead to a more diverse candidate pool.[12] However, successfully removing unconscious bias in this way would require both the algorithm and the data set it is analyzing to be unbiased.[13] Regardless of how well the algorithm is coded, its functional efficacy will depend on having an unbiased data set for that algorithm to process.

The difficulties in having an unbiased data set are further complicated by the "black box" problem. A "black box" is a computing term used to describe "a device, system or program that allows you to see the input and output, but gives no view of the processes and workings between. "The AI black box, then, refers to the fact that with most AI-based tools, we don't know how they do what they do."[14] Black boxes are inherent in machine learning and are derivatives of the algorithms serving their coded functions.[15] Even if some black boxes could be cracked, there are downsides to transparency. The absence of a black box allows insight into how things work inside the algorithm; but, "if the world can figure out how your AI works, it can figure out how to make it work without you."[16] Companies have also invoked IP protections to keep their black boxes from becoming any less opaque partly because many firms have an economic interest in protecting their algorithms.[17]

AI and employment practices will continue to overlap with the use of algorithmic processing and data-mining techniques in human resources. People or workforce analytics "is an approach to human resources management" that utilizes big data to capture insights about job performance, as opposed to subjective assessment by managers.[18] It is clear that predicting who would make an equitable and unbiased future employee based on the

12. *Id.* at 530.

13. *Id.* at 533.

14. *The AI Black Box Problem*, THINK AUTOMATION, https://www.thinkautomation.com/bots-and-ai/the-ai-black-box-problem/ (last visited Mar. 4, 2021).

15. Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J. L. & TECH. 889, 897 (2018).

16. Tristan Greene, *Researchers Were About to Solve AI's Black Box Problem, Then the Lawyers Got Involved*, THE NEXT WEB, (Dec. 17, 2019), https://thenextweb.com/artificial-intelligence/2019/12/17/researchers-were-about-to-solve-ais-black-box-problem-then-the-lawyers-got-involved/.

17. *Id.*

18. Matthew T. Bodie et al., *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 961, 964 (2017).

qualities of existing employees is challenging.[19] People analytics "runs the risk of homosocial reproduction . . . either because of the data that the predictive model comes from or because the designer uses labels or characteristics based on a sense of what made him or herself a good worker."[20] That is to say, the same human discretion and policy choices that have created the existing data pool can find ways of permeating how an algorithm distinguishes a good candidate from a bad candidate.

B. DISCRIMINATION CLAIMS UNDER AMERICAN LAW

In the early 1960s, the world watched as the United States grappled with the millions of Americans that demanded that the government deliver on the promises of equal protection under the 14th Amendment. Largely as a response to the Civil Rights Movement, Congress passed an omnibus bill addressing discrimination in voting, education, and employment among other things.[21] Specifically, Title VII of the Civil Rights Act of 1964 made it illegal to discriminate against . . . or . . . to limit, segregate, or classify" an applicant or employee because of their "race, color, religion, sex, or national origin."[22] This law is the broadest federal statute prohibiting discrimination in the United States, with interpretation and enforcement of Title VII turning the statute "into a vehicle for social reform that equalized access to the courts by allowing employees to take action against private employers' discriminatory practices."[23]

There are two theories upon which discrimination claims are made today: disparate treatment or disparate impact. Disparate treatment prohibits reliance on any of these protected identity characteristics in making employment decisions[24] and employment decisions "made in reliance upon stereotypes about protected characteristics."[25] This basis requires a finding of

19. *Id.* at 1013.

20. *Id.*

21. Brandon Haase, *Guaranteeing the Right to Vote for Twenty-First Century America*, 43 J. LEGIS. 240, 241 (2016).

22. 42 U.S.C. § 2000e-2(a)(1)–(2) (2018).

23. Wendy B. Scott et al., *The Influence of Justice Thurgood Marshall on the Development of Title VII Jurisprudence*, 89 ST. JOHN'S L. REV. 671, 672 (2015).

24. Bodie, *supra* note 18, at 1009.

25. Joseph Blass, Note, *Algorithmic Advertising Discrimination*, 114 NW. U. L. REV. 415, 443 (2019).

"discriminatory intent[,]"[26] meaning that the plaintiff must prove that the employer had an intent to discriminate against them based on a protected class or stereotypes about a protected class in order to make a claim of disparate treatment. Plaintiffs must show that they are members of a Title VII protected class,[27] that they are qualified for the position at issue, "and that similarly situated employees were treated differently."[28] Disparate treatment cases are evaluated under the McDonnell Douglas burden-shifting framework, which requires that the plaintiff-employee establish a prima facie case. If the defendant-employer provides evidence of a legitimate, non-discriminatory reason for the employment decision, the plaintiff must show that, despite the employer's non-discriminatory reason, an inference of discrimination still exists..[29]

The disparate impact theory, on the other hand, bars neutral practices that negatively impact members of protected groups, regardless of whether the reasons for such practices are identifiable or not.[30] The disparate impact basis of discrimination was first accepted by the Supreme Court in *Griggs v. Duke Power Co.*[31] Disparate impact claims, as opposed to disparate treatment claims, do not require the plaintiff to identify discriminatory intent, but rather an internal practice or process that results in a discriminatory effect.[32] Thus, an employer can be liable for discrimination if a process or practice of theirs results in discrimination even in the absence of specific discriminatory intent.

C. GLOBAL PERSPECTIVE: EXISTING REGULATIONS OF ARTIFICIAL INTELLIGENCE

Other nations have already begun to grapple with the effects of artificial intelligence with varying responses. Eighteen countries have already launched their own national AI

26. *Id.* at 442.

27. 42 U.S.C. § 2000e-2(a)(1)–(2) (2018).

28. Joseph Seiner, *Disentangling Disparate Impact and Disparate Treatment: Adapting the Canadian Approach*, 25 YALE L. & POL'Y REV. 95, 105 (2006).

29. McDonnel Douglas Corp. v. Green, 411 U.S. 792, 802 (1973); *accord* Salter v. Alltel Communs., Inc., 407 F. Supp. 2d 730, 734–35 (E.D.N.C. 2005).

30. Steiner, *supra* note 28, at 99.

31. Griggs v. Duke Power Co., 401 U.S. 424, 430 (1971).

32. Seiner, *supra* note 28 at 100.

initiatives, with half including new sources of funding providing anywhere between $20 million and $2 billion.[33] Jason Furman, a Harvard professor who served on President Obama's Council of Economic Advisors and aided in drafting the Obama Administration's report on AI, said that an AI initiative needs "concrete commitments—not just promises—in order to fulfill its stated goals."[34] While the Biden Administration has inherited a freshly minted National AI Initiative Office and increased funding for research initiatives established by the outgoing President,[35] research groups, industry groups, and some members of Congress are already stressing the importance of international cooperation, specifically with Europe, in setting standards for AI that shape ethical and globally beneficial development of the technology.[36] If the U.S. wishes to remain a global leader in AI technology, it will need to work cooperatively with its international allies.

In 2014, Stanford University began an initiative dedicated to understanding and anticipating how the growing integration of AI into our lives will impact our legal norms and frameworks.[37] In a 2016 report, the group did not seem optimistic about a comprehensive solution to AI being generated by administrative agencies or Congress in the near future.[38] The report referred to a pre-GDPR study that yielded counterintuitive results; countries with detailed regulations

33. James Vincent, *Trump Signs Executive Order to Spur U.S. Investment in Artificial Intelligence*, VERGE (Feb. 11, 2019), https://www.theverge.com/2019/2/11/18219981/american-ai-initiative-trump-administration-funding-research-data.

34. *Id.*

35. Press Release, Office of the President of the United States, Office of Science and Technology Policy, *The White House Launches the National Artificial Intelligence Initiative Office* (Jan. 12, 2021), https://trumpwhitehouse.archives.gov/briefings-statements/white-house-launches-national-artificial-intelligence-initiative-office/.

36. Steven Overly & Melissa Heikkilä, *China Wants to Dominate AI. The U.S. and Europe Need Each Other to Tame It*, POLITICO (Mar. 2, 2021), https://www.politico.com/news/2021/03/02/china-us-europe-ai-regulation-472120; *see also* Joshua P. Meltzer & Cameron F. Kerry, *Strengthening International Cooperation on Artificial Intelligence*, BROOKINGS (Feb. 17, 2021), https://www.brookings.edu/research/strengthening-international-cooperation-on-artificial-intelligence/.

37. STANFORD UNIV., ONE HUNDRED YEAR STUDY ON ARTIFICIAL INTELLIGENCE (AI100), A.I. & LIFE IN 2030 1 (Sept. 2016), https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.

38. *Id.* at 48.

"bred a 'compliance mentality'" that incentivized companies to act simply to evade harsh penalties and compliance with the detailed mandate of the law.[39] Countries with broader, less specific goals "encouraged companies to develop a professional staff and processes to enforce privacy controls, engage with outside stakeholders, and to adapt their practices to technology advances."[40] This created what the report described as a "virtuous cycle of activity involving internal and external accountability, transparency, and professionalization, rather than narrow compliance."[41] Though not nearly as expansive as the GDPR, the U.S. has some data protection frameworks, but the models are often narrow or largely sector- and state-specific.[42]

1. GDPR: History

The General Data Protection Regulation is the "primary law regulating how companies protect EU citizens' personal data."[43] While the GDPR felt like a major turning point for American companies, it is actually just a strengthened iteration of earlier EU Directives.[44] Generally, Europeans have broader notions of privacy, especially as it pertains to data.[45] While stricter data privacy standards had been the norm in Europe, the GDPR taking effect greatly expanded who the GDPR applied to, and in what capacity.

The GDPR requires not only EU member states, but all companies that market goods or services to residents of the EU, regardless of their location, to comply with its mandates.[46] Article 5 outlines the foundational principles of the regulation: "(1) lawfulness, fairness and transparency, (2) purpose limitation, (3) data minimization, (4) accuracy, (5) storage

39. *Id.*
40. *Id.* at 49.
41. *Id.* at 48–49.
42. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 258 (2016).
43. Juliana De Groot, *What is the General Data Protection Regulation? Understanding and Complying with GDPR Requirements in 2019*, DIGITAL GUARDIAN (Dec. 2, 2019), https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection.
44. MCGEVERAN, *supra* note 42, at 258.
45. *Id.* at 269.
46. *Id.*

limitation, (6) security and (7) accountability."[47] While these principles are not strict rules, they "embody the spirit of the protection regime," and carry hefty administrative fines up to €20 million, or 4 percent of the offending companies' total worldwide annual turnover for violations.[48] Thus, the emphasis on fairness in the GDPR is significant in that it attempts to address the effect of big data on individuals. "[49]

2. GDPR: Structure & Important Rights

The Article 5 principles are one of four basic pillars that outline the considerations companies should take into account to handle data. The second major pillar is that companies need explicit and specific purposes to allow for the handling of personal data.[50] It is important to note that this is separate from the guiding principles in Article 5. Rather, an Article 6 basis is required to handle the data at all. Article 6 requires that there be a lawful basis for data processing—meaning that the reason to collect and process information must have a basis enumerated by law.[51] In fact, Article 9 outlines more stringent requirements, such as heightened consent, for certain subcategories of personal data that are considered especially sensitive.[52]

The third major pillar of requirements dictates that companies must create organizational structures and policies that promote responsible data privacy practices.[53] This pillar dictates not only what companies must do to create a structure to handle data responsibly, but also sets up standards for data protection when that data is transferred across borders, like into the United States, where data protection requirements are much less stringent.[54]

The final pillar involves the immense number of individual data subject rights that the GDPR creates for individual data

47. *The Principles*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (last visited June 26, 2021).

48. *Id.*

49. Michael Butterworth, *The ICO and Artificial Intelligence: The Role of Fairness in the GDPR Framework*, 34 COMPUT. L. & SEC. REV. 257, 259 (2018).

50. MCGEVERAN, *supra* note 42, at 258.

51. GDPR, *supra* note 8, art. 6.

52. *Id.* art. 9.

53. MCGEVERAN, *supra* note 42, at 258.

54. *See* GDPR, *supra* note 8, art. 3.

subjects. The GDPR creates a number of individual data rights, such as the right to object,[55] the right to rectification,[56] and the right to data portability.[57] These rights to access and control of personal data are much more expansive under the GDPR than any regime in the U.S. Perhaps because of its recent overhaul, GDPR Article 22 directly addresses "data subjects' rights and companies' obligations when personal data is used in a narrow category of automated decision-making . . . Article 22 creates a right not to be subject to certain types of automated decision, [and] outlines three exceptions to that right, and mandates safeguards for the exceptions."[58] Under Article 22, data subjects have rights related to automated decision-making and profiling, including the right to ask and demand an explanation of how a decision was made and the right to ask for a human to intervene and review the results of the automated data processing.[59] The GDPR defines profiling as "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyze or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements[.]"[60]

Despite the GDPR being lauded as a necessary check on the growing power of tech companies,[61] the U.S. remains without any strong data privacy regulations.[62] While the GDPR does impact American companies—especially tech behemoths such as

---

55. *Id.* art. 21.

56. *Id.* art. 16.

57. *Id.* art. 20.

58. Emily Pehrsson, *The Meaning of the GDPR Article 22*, 4 (Eur. Union L. Working Papers No. 31, 2018), https://www-cdn.law.stanford.edu/wp-content/uploads/2018/05/pehrsson_eulawwp31.pdf.

59. *Rights Related to Automated Decision Making Including Profiling*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/ (last visited June 28, 2021).

60. GDPR, *supra* note 8, recital 71.

61. Adam Satariano, *Google is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

62. Derek Hawkins & Bastien Inzaurralde, *The Cybersecurity 202: Why a Privacy Law like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST: POWERPOST (May 25, 2018, 8:14 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/.

Facebook, Apple and Google—the law is not legally binding in the United States.[63] Americans lack the same recourse as an EU citizen or resident if they believe that their data rights have been violated.[64] "Legislation to create a federal standard for how companies and agencies report data breaches . . . has repeatedly dead-ended[.]"[65] It has been argued that a similar law would be a tough sell in the United States, given that there is no single agency for enforcement on the federal level, and a powerful tech lobby influencing an already challenging legislative environment.[66] Some companies, like Facebook, have formed ethics teams to prevent bias in AI technologies.[67] However, "since the dawn of the Industrial Revolution, no major industry has successfully regulated every aspect of its operations completely by itself. It would be naive to think the first success case will emerge now."[68]

III. LEGAL RISKS ARISING FROM USE OF AI IN HIRING

Disparate impact claims, as opposed to disparate treatment claims, do not require proof of discriminatory intent.[69] Instead, plaintiffs must show that a facially neutral employment practice disproportionately and adversely impacts a protected group.[70] Under the disparate impact theory, a "plaintiff can prevail in a lawsuit by establishing an employer's policy or practice affects members of the protected group so disproportionately that the court can infer discrimination from that impact."[71] The Supreme

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. *See, e.g.*, Jordan Novet, *Facebook Forms a Special Ethics Team to Prevent Bias in its A.I. Software*, CNBC https://www.cnbc.com/2018/05/03/facebook-ethics-team-prevents-bias-in-ai-software.html (May 3, 2018, 11:52 AM).

68. Brad Smith & Carol Ann Browne, Tech Firms *Need More Regulation*, ATLANTIC (Sept. 9, 2019), https://www.theatlantic.com/ideas/archive/2019/09/please-regulate-us/597613/.

69. Seiner, *supra* note 28, at 99.

70. *See, e.g.*, *Questions and Answers on EEOC Final Rule on Disparate Impact and "Reasonable Factors Other Than Age" Under the Age Discrimination in Employment Act of 1967*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/regulations/questions-and-answers-eeoc-final-rule-disparate-impact-and-reasonable-factors-other-age (last visited June 26, 2021).

71. Sarah Smith Kuehnel et al., *Unintentional Discrimination? What Every*

Court's decision in *Wards Cove Packing Co. v. Antonio* established that the plaintiff bears the burden of "isolating and identifying the specific employment practices that are allegedly responsible for any observed statistical disparities."[72] Beyond a simple disparity between minority and non-minority employees, plaintiffs must demonstrate that the statistical imbalance is a result of a facially neutral policy or practice.[73] In *International Brotherhood of Teamsters v. United States*, the Supreme Court emphasized the importance of statistics in employment discrimination cases:

> Statistics showing racial or ethnic imbalance are probative in a case such as this one only because such imbalance is often a telltale sign of purposeful discrimination; absent explanation, it is ordinarily to be expected that nondiscriminatory hiring practices will in time result in a work force more or less representative of the racial and ethnic composition of the population in the community from which employees are hired. Evidence of long-lasting and gross disparity between the composition of a work force and that of the general population thus may be significant even though . . . Title VII imposes no requirement that a work force mirror the general population.[74]

In assessing disparate impact of policies, the Equal Employment Opportunity Commission (EEOC) uses a "four-fifths rule of thumb" standard.[75] This standard has been referred to as a "ratio of ratios" since it requires dividing: (1) the percentage of protected class members who were qualified by (2) the percentage of "the most successful group's selection rate."[76]

Statistical analysis is regarded as an important tool of

Employer Needs to Know About Disparate Impact Claims, OGLETREE DEAKINS (May 22, 2018), https://ogletree.com/insights/2018-05-22/unintentional-discrimination-what-every-employer-needs-to-know-about-disparate-impact-claims/.

72. Wards Cove Packing Co. v. Antonio, 490 U.S. 642, 656 (1989) (quoting Watson v. Fort
Worth Bank & Trust, 487 U.S. 977, 994).

73. *Id.* at 645–46.

74. International Brotherhood of Teamsters v. United States, 431 U.S. 324, 339 n.20 (1977).

75. Kuehnel, *supra* note 71.

76. *Id.*

analysis for recognizing disparate impact theory claims. This is seen in *Griggs v. Duke Power Co*., a quintessential case in which the Supreme Court recognized disparate impact claims as a basis of a discrimination.[77] The employer, which openly discriminated against African Americans before Title VII was passed, created a new policy that required job applicants to have high school diplomas.[78] The Court found that this mechanism, while facially neutral, had a discriminatory impact because twelve percent of African American males possessed high school diplomas, versus thirty-four percent of similarly situated white males at the time.[79] The Court identified the touchstone to a disparate impact case as a show of business necessity, allowing defendant-employers to subvert liability by demonstrating that the discriminatory practice was related to the nature or function of the job or business.[80]

Despite recognizing the basis of disparate impact in *Griggs*, the Court outlined specific instructions that dampened plaintiff's rights in *Wards Cove Packing Co. v. Antonio*.[81] In *Wards Cove,* the Supreme Court reviewed a disparate impact claim against a cannery facility operating in Alaska that employed mostly white employees in the jobs with higher pay and better benefits.[82] An analysis of disparate impact after the split *Wards Cove* decision required that "plaintiffs . . . identify the 'specific or particular employment practice' that resulted in the disparate impact . . . [and] the defendant's policy justification would be subject to only a 'reasoned review' . . . [and] the burden of proof would 'remain[] with the plaintiff at all times.'"[83] In an attempt to steer disparate impact analysis away from hiring quotas, the *Wards Cove* Court chilled the expanded disparate impact basis recognized in *Griggs*.[84]

Shortly after the *Wards Cove* decision, Congress passed the Civil Rights Act of 1991, amending Title VII and codifying disparate impact basis of discrimination.[85] Congress clarified that the a discriminatory impact claim (1) "must identify the

77. Griggs v. Duke Power Co., 401 U.S. 424, 430 (1971).
78. *Id.* at 426–27.
79. *Id.* at 430 n.6.
80. *See* Seiner, *supra* note 28, at 100.
81. *Id.* at 101–102.
82. *Id.* at 101.
83. *Id.* at 102 (quoting Wards Cove Packing Co. v. Antonio, 490 U.S. 642, 657, 659 (1989)).
84. *See id.* at 101.
85. *Id.* at 102–03.

particular employment practice resulting in the impact, unless the policy or practice is 'not capable of separation for analysis[,]'"[86] (2) the burden of proving business necessity rests with the defendant,[87] and (3) the employee can still overcome the employer's showing of business necessity by showing that there are less discriminatory, alternative practices that achieve the same business goals.[88] Thus, the disparate impact claims are evaluated in a similar burden-shifting framework as the disparate treatment-based claims. For example, a disparate impact claim was unsuccessful in *Griggs* because there were less African Americans hired than the most successful groups.[89] Courts require a specific business reason for the discriminatory policy or practice in order to counter a plaintiff's prima facie case based on business necessity: "a valid business justification must 'serve[], in a significant way, the legitimate employment goals of employer.'"[90] Thus, screening requirements like high school diplomas can have valid business justifications for their enforcement, but only if the requirement is related to or necessary for the applicant or employee to engage the job functions. In *Griggs*, requirements of a high-school diploma served no such function given the type of work that the defendant-employer was hiring for.

A. THE INCREASED USE OF AI IN THE EMPLOYMENT SETTING WILL POSE NEW CHALLENGES IN ANALYZING AND ARGUING DISPARATE IMPACT DISCRIMINATION CLAIMS.

Title VII claims based on disparate impact theory depend on statistical analysis of applicant pools and those that go on to become employees. The business judgment justification can alternatively rely on the employer's ability to articulate a business reason, or explanation of their policy. However, employers will have more problems articulating a statistical analysis or reasoning behind its business necessity if they base their business decisions on the outcomes of a "black box" AI algorithm. Research from Manish Raghavan and other computer and information science scholars has "found [that] companies tend to favor obscurity over transparency in this emerging field,

86. *Id.* (quoting 42 U.S.C. § 2000e-2(k)(1)(B(i) (2000)).
87. *Id.*
88. *Id.*
89. *See* Griggs v. Duke Power Co., 401 U.S. 424, 429–30 (1971).
90. Kuehnel, *supra* note 71.

where lack of consensus on fundamental points—formal definitions of 'bias' and 'fairness,' for starters—have enabled tech companies to define and address algorithmic bias on their own terms."[91] In their study, the scholars documented and analyzed the claims and practices of eighteen companies currently in the business of offering algorithm-based solutions for employment assessments, with a particular emphasis on vendors of pre-employment assessments.[92] The researchers found that "[v]ery few vendors offer[ed] concrete information about how they validate[d] their assessments or disclose[d] specifics on how they mitigate algorithmic bias[.]"[93] While some companies market their products as providing a less biased method of making hiring decisions, Raghavan analogized between the "reduction in bias," or use of the word "fairness," and eggs labeled "free range" and explained that "[t]here is a set of conditions under which eggs can be labeled free range, but our intuitive notion of free range may not line up with those conditions."[94] While artificial intelligence has been marketed and understood as a way of reducing human bias in hiring, the purported resulting increase in fairness may not be what businesses are expecting.

Artificial intelligence has already led to some undesirable, biased results when used in a hiring context. Amazon, the world's largest retailer,[95] had a computer-based intelligence program that reviewed job applicants' resumes "with the aim of mechanizing the search for top talent[.]"[96] Amazon's system, based on how it was programmed, was generating results with a

---

91. Louis DiPietro, *Are Hiring Algorithms Fair? They're Too Opaque to Tell, Study Finds*, CORNELL CHRONICLE (Nov. 20, 2019), http://news.cornell.edu/stories/2019/11/are-hiring-algorithms-fair-theyre-too-opaque-tell-study-finds.

92. Manish Raghavan et al., *Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practice*, ASS'N FOR COMPUTING CONF. ON FAIRNESS, ACCOUNTABILITY, & TRANSPARENCY 5 (Dec. 6, 2019) https://arxiv.org/pdf/1906.09208.pdf.

93. Louis DiPietro, *supra* note 91.

94. *Id.*

95. Lauren Debter, *Amazon Surpasses Walmart as the World's Largest Retailer*, FORBES (May 15, 2019, 5:50 PM), https://www.forbes.com/sites/laurendebter/2019/05/15/worlds-largest-retailers-2019-amazon-walmart-alibaba/#7d1d42b44171.

96. 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-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

preference against women.[97] Specifically, the algorithm penalized candidates that had the word "women's" on their resume (like Women's Business Association, etc.), and downgraded those applicants that had graduated from two all-women's colleges.[98] Ultimately, the project was abandoned because, while the company attempted to edit these biased tendencies, there was no way to guarantee that the algorithm would not be discriminatory in the future.[99] As evidenced by Amazon, bias can clearly carry over to algorithms—but discerning intent from impact alone is more challenging in the context of artificial intelligence. Clearly, as some business scholars have opined, there are substantial gaps in applying AI to human resource management, specifically pointing to the legal constraints resulting from an inability to explain results.[100] This will pose significant challenges for both plaintiff-employees and defendant-employers.

1. Changes for Plaintiff-Employees

People analytics is the practice of applying algorithms programmed to find patterns in a sea of data.[101] The data is any point of information about a person—where they live, groups they follow on social media, things they shop for.[102] These data points become the basis of the outcomes of the algorithms, which inform employment decisions.[103] For example, data driven job advertising strategies can often lead to disparate results.[104] While an algorithm may not filter based on racial group directly, it might create patterns based on membership of racial affinity groups, which would likely be considered a facially neutral practice.[105] Another example is that targeted advertising might

97. *Id.*
98. *Id.*
99. *Id.*
100. Prasanna Timbe et al., *Artificial Intelligence in Human Resource Management: Challenges and a Path Forward* 61 CAL. MGMT. REV. 15, 16 (2019).
101. Bodie et. al., *supra* note 18, at 964.
102. Raub, *supra* note 11, at 535–36.
103. Rebecca Heilweil, *Artificial Intelligence Will Help Determine If You Get Your Next Job*, VOX: RECODE (Dec. 12, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/12/20993665/artificial-intelligence-ai-job-screen.
104. *See, e.g.*, Dastin, *supra* 96.
105. Bodie et al., *supra* note 18, at 1014.

prefer certain zip codes; while geographic proximity could be a reasonable business consideration, targeting based on ZIP code can lead to disparate results because this data point is often correlated with race.[106] This is a recognized pattern in which algorithms, though programmed to ignore protected characteristics like race, begin to process proxy categories for the protected characteristic, like ZIP code. Thus, it can be difficult as a plaintiff to point to a policy that has a discriminatory effect because a seemingly innocuous geographic setting can lead to biased results without any discriminatory intent whatsoever.

There is an added risk of classification bias, which "occurs when employers rely on classification schemes, such as data algorithms, to sort or score workers in ways that worsen inequality or disadvantage along the lines of race, sex or other protected characteristics."[107] Classification bias is uniquely exacerbated by algorithmic processing because the nature of algorithmic processing includes continuous categorization of candidates based on their data inputs.[108] Professor Pauline Kim has argued that this sort of data mining is distinct from the sorts of employment tests or sorting mechanisms executed by people because "data mining models often rely on 'discovered' relationships between variables rather than measuring previously identified job-related skills or attributes."[109] Thus, it will be more difficult for plaintiffs in disparate treatment cases to point to an inherently biased algorithm. While it may still be possible to make a disparate impact claim, disparate treatment claims under Section 1981 may have longer statutes of limitations and lead to higher penalties despite having a higher bar.[110] It will be challenging to prove discriminatory intent, especially if the algorithm is *known* to be biased.[111]

Biased outcomes from AI may lead to challenges in evaluating discrimination claims. In claims that arise from employment decisions that are based on an algorithm's analysis, it may be difficult for plaintiffs to point to a specific "policy or

106. *Id.*

107. Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 866 (2017).

108. *Id.*

109. *Id.* at 908.

110. Eric Bachman, *5 Differences Between Title VII and Section 1981 That Can Help Your Employment Race Discrimination Case*, VII Nat. L. Rev., no. 163 (Jun. 12, 2017).

111. *See Id.* ("Section 1981, on the other hand, outlaws only intentional discrimination.").

procedure" that is causing the disparate impact, because the causecould be any combination of a number of ambiguous factors.[112] While a company or programmer may intend for an algorithm to operate in one way, there is no way to truly understand why an output is generated because of the inherent black box problem. This lack of understanding of why an algorithm generates the results it does exacerbates existing power issues.[113] Notably, the data revolution has "led to an imbalance in powers among the actors on the data-driven markets. This is particularly troubling in the context of employment, where an employer typically has much more power over personal data than an employee."[114]

2. Changes for Defendant-Employers?

Despite the disadvantages for plaintiffs, the lack of clarity on the machinations and exact causes of why certain results are derived may pose significant challenges for employers to manage their legal risk and support their defenses. The "black box" problem can impact employers' ability to make a business necessity defense.[115] While employers can often control either the algorithm's objectives and some of the data inputs, employers may not be able to explain why the algorithm ultimately led to the decision it did.[116] This will make justifying business decisions challenging because despite the control that employers have, they are as limited in their understanding of "why" an algorithm has made a decision as an app design engineer would be. While this opacity can act as a shield to liability, it also obfuscates a company's ability to explain business reasoning. A company could be held liable for employing an algorithm that, for whatever reason, led to biased

112. FRANK PASQUALE, THE BLACK BOX SOCIETY 23 (2015).

113. *Id.*

114. Bart Custers & Helena Ursic, *Worker Privacy in a Digitalized World Under European Law*, 39 COMPAR. LAB. L. & POL'Y J. 323, 339 (2018).

115. *See* Bryan Lufkin, *Why the Biggest Challenge Facing AI is an Ethical One*, BBC: FUTURE (Mar. 7, 2017), https://www.bbc.com/future/article/20170307-the-ethical-challenge-facing-artificial-intelligence.

116. Ensuring a Future That Advances Equity in Algorithmic Employment Decisions: Hearing Before the Civ. Rts. & Hum. Servs. Subcomm., H. Comm. on Educ. and Lab., 116th Cong. 4 (2020) (Statement of Jenny R. Yang, Senior Fellow, Urban Institute), https://edlabor.house.gov/imo/media/doc/YangTestimony02052020.pdf.

patterns in a company's hiring process. As Professor Kim has pointed out, "the differences between employment testing and data mining also mean that defenses based on Section 703(h) of Title VII do not apply."[117] Section 703(h) currently shields employers from liability when they use a "professionally developed ability test", as long as that test does not discriminate, either in fact or in impact, based on a protected characteristic.[118]

There is also ambiguity surrounding the question of liability. In the past few years, there has been an increase in the number of firms offering to provide people and workforce analytics that help in all phases of the employment process. LinkedIn uses an internal artificial intelligence that ranks candidates for jobs, ZipRecruiter uses AI to match candidates by geographic proximity and qualification, while third-party platforms like Arya use machine learning to mine a client-company's internal database and the greater internet to identify and screen candidates.[119]

Employers may incur liability for blind reliance on an algorithmic analysis that is touted as being less biased and more efficient.[120] None of the external vendors have been willing to indemnify their employer-customers in the very possible scenario that a vendor's algorithm is questioned in a litigation action.[121] In this way, it is unclear the extent to which employers can truly rely on these technologies to be reliably less biased and more efficient, especially when considering the legal risk that would come with adoption of such technologies.

IV. DATA PRIVACY REGULATION MODEL

Despite being home to almost half of the world's largest tech companies,[122] the United States lacks a national consumer data

117. Kim, *supra* note 107, at 908.

118. *Id.*

119. Heilweil, *supra* note 103.

120. Ben Dattner et al., *The Legal and Ethical Implications of Using AI in Hiring*, HARV. BUS. REV. (Apr. 25, 2019), https://hbr.org/2019/04/the-legal-and-ethical-implications-of-using-ai-in-hiring.

121. Chris Opfer, *AI Hiring Could Mean Robot Discrimination Will Head to Courts*, BLOOMBERG L. (Nov. 12, 2019, 5:01 AM), https://news.bloomberglaw.com/daily-labor-report/ai-hiring-could-mean-robot-discrimination-will-head-to-courts ("The manufacturers are saying, 'We will help insulate you from a bias, but, by the way, we're not responsible for any liability if you get sued.'").

122. Jonathan Ponciano, *The Largest Technology Companies in 2019: Apple*

protection law. "Virtually the only developed nation without a comprehensive consumer data protection law and an independent agency to enforce it."[123] Harvard professor of law and computer science Jonathan Zittrain has pointed to the early days of the Internet, the late 1990s and early 2000s, when there seemed to be a global sense "about not wanting to kill the goose laying the golden eggs."[124] Others have noted that "Americans have almost no safeguards for apps, in part because Congress has never established an agency to policy Facebook, Instagram, Uber, YouTube and other online services that use sophisticated data-mining tools to surveil, sort and steer people on a massive scale."[125] The regulatory agency most often regulating data-related tech crimes is the Federal Trade Commission, overstretched with limited and specific powers, by way of its responsibility to police "deceptive and unfair trade practices."[126] Perhaps due to a number of high-profile data protection failures at tech giants, consumer groups and U.S. Congress members are calling for the enactment of sweeping data protection laws and creation of the dedicated regulatory agency to enforce those laws.[127] The U.S.'s policies regarding the internet and big tech are in need of an overhaul. In order to understand what a model focused on data protection is, one must first consider the most comprehensive data privacy regime in the world: the GDPR.

A. WHAT IS THE GDPR'S APPROACH?

The GDPR took force in May of 2018, putting into effect the strictest data privacy regulations in the world.[128] Similar to the

Reigns as Smartphones Slip and Cloud Services Thrive, FORBES (May 15, 2019, 5:50 PM) (noting that 65 of 154, or approximately 42%, of 2019's biggest tech companies were American).

123. Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html.

124. *Why Europe Is Willing to Regulate Tech More Than the U.S.*, NAT'L PUB. RADIO (Jan. 2, 2018, 4:13 PM), https://www.npr.org/2018/01/02/575168206/why-europe-is-willing-to-regulate-tech-more-than-the-u-s.

125. Singer, *supra* note 123.

126. *Id.*

127. *Id.*

128. Matt Burgess, *What is the GDPR? The Summary Guide to GDPR Compliance in the UK*, WIRED (Mar. 24, 2020, 4:30 PM), https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

current U.S. position on artificial intelligence,[129] the European Union had found itself with outdated rules, created in the 1990s, that had failed to keep pace with the technological changes of the time.[130] It was in light of this realization that the European Union created the GDPR which, by way of regulating data, as one of two key ingredients to artificial intelligence, regulates artificial intelligence.[131] Mandatory GDPR compliance applies not only to those companies within the European Union, but any firms not located in the EU, if they offer free or paid goods or services to EU residents **or** monitor the behavior of EU residents.[132] For employers, the broad definition of "processing data" can mean "everything from receiving resumes to archiving emails to conducting employee performance reviews and more."[133] In this way, the GDPR's reach, especially on artificial intelligence, already extends to many firms operating in the U.S., despite the assertion that the American AI Initiative directives mostly encourage innovation without setting up regulations that "needlessly" get in the way.[134] While the GDPR does impose regulations on companies that may slow AI advances,[135] "[t]hese regulations establish a road map for how companies should handle personal data and protect customer privacy."[136] These regulations also "encourage companies to build privacy standards into their products from the start—known as 'privacy by design.'"[137] The GDPR, while introducing regulatory mechanisms that have been criticized for slowing innovation, ended an era that was known as the "wild west era" for data privacy.[138] While the EU's policies seem much stricter,

129. *See* Rebecca Heilweil, *supra* note 103 (discussing the inadequacy of state and federal regulations of employment use of AI).

130. Burgess, *supra* note 128.

131. *See* Oleg Rogynskyy, *What GDPR Means for Businesses with an AI Strategy*, FORBES: TECH. COUNCIL (Sept. 6, 2019, 9:45 AM), https://www.forbes.com/sites/forbestechcouncil/2019/09/06/what-gdpr-means-for-businesses-with-an-ai-strategy/#7ab9c065858d.

132. GDPR, *supra* note 8, art. 3.

133. Ashik Ahmed, *Employee Data Privacy in the GDPR Era: What You Should Know*, FORBES (May 2, 2018, 9:36 AM), https://www.forbes.com/sites/ashikahmed/2018/05/02/employee-data-privacy-in-the-gdpr-era-what-you-should-know/#6097a95c5c83.

134. *See* Hawkins & Inzaurralde, *supra* note 62 (noting that American firms will have to comply with the GDPR).

135. Rogynskyy, *supra* note 131.

136. *Id.*

137. *Id.*

138. *We Need to Fix the 'Data Wild West'*, PRIV. INT'L (Feb. 4, 2019),

U.S. governmental and legal institutions can borrow principles from the GDPR to adapt existing frameworks to emerging tech challenges. Specifically, the GDPR creates rights of control, rights of access, and rights against decisions made on the basis of data collection and processing.

1. Transparency and Fairness

Article 5(1) of the GDPR states that "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, and transparency')[.]"[139] One must satisfy all three of the elements: lawfulness, more closely defined in Articles 6 to 10; transparency, with more explanation in Articles 13 and 14; and fairness.[140] Articles 13 and 14 establish an individual's right to be informed, and require that data processing subjects be provided information about the lawful basis for processing in a privacy notice.[141]

Under Article 21 of the GDPR, individual data subjects can "object . . . to profiling that is necessary . . . for the performance of a task that is carried out in the public interest or in the exercise of official authority vested in the controller[.]"[142] In this way, the GDPR forces a balancing between the often competing interests of the controller of the profiling mechanism (in the employment world, this would be an employer or third-party contractor to the employer) and the subject.[143] Essentially, the GDPR guarantees a semblance of transparency and gives applicants and employees a legitimate, enforceable basis for objection.[144]

The United States could benefit from enacting a similar tenant enforcing emphasis on transparency. This emphasis on transparency could help to alleviate some of the "black box" problems, given that most "black boxes" are not compliant with

---

https://privacyinternational.org/long-read/2677/we-need-fix-data-wild-west.

139. GDPR, *supra* note 8, art. 5.

140. *Principle (a): Lawfulness, Fairness and Transparency*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/ (last visited June 27, 2021).

141. GDPR, *supra* note 8, arts. 13–14.

142. Marta Otto, *"Workforce Analytics" v Fundamental Rights Protection in the EU in the Age of Big Data*, 40 COMPAR. LAB. L. & POL'Y J. 389, 396–97 (2019).

143. *Id.* at 403.

144. *Id.* at 396.

EU data protection laws.[145] As Raghavan found, while many vendors that the scholar group encountered in their research at least acknowledged the risk of bias and are taking steps to mitigate the ill-effects that could result, there was "a notable lack of consensus or direction on exactly how this should be done."[146] Even an American membership association, the Society for Human Resource Management, has advised that U.S. employers that are covered by the GDPR to be transparent by providing employees and job applicants with notice that includes "[W]hy the data is being collected [,] [H]ow long the data will be retained [, and] [H]ow employees can go about getting the data they want to see."[147]

2. Data Protection

The GDPR also brings a data protection element that is favorable to employees as data subjects. Under the GDPR, an entity that wishes to process data of an individual, or employee, must have at least one of six lawful bases for processing that data: (1) consent, (2) contract, (3) legal obligation, (4) vital interests, (5) public task, or (6) legitimate interests.[148] Even if a company has no actual location within the European Union, the GDPR "applies to the processing of personal data . . . whether the processing takes place in the Union or not."[149] Many of these lawful bases rely on the data processing to be "necessary." Interpretation of the mandates of the GDPR have been left to each individual member-country's enforcement agency.[150] The UK Information Commissioner's Office has clarified that while "necessary" does not require the data processing in question to be absolutely essential, it "must be more than just useful, and

145. Warwick Ashford, *GDPR a Challenge to AI Black Boxes*, COMPUTERWEEKLY.COM (Nov. 8, 2018, 1:35 PM), https://www.computerweekly.com/news/252452183/GDPR-a-challenge-to-AI-black-boxes.

146. DePietro, *supra* note 91.

147. Allen Smith, *Three GDPR Compliance Steps Explained*, SOC'Y FOR HUM. RES. MGMT. (May 15, 2018), https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/3-gdpr-compliance-steps-explained.aspx.

148. *Lawful Basis for Processing*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ (last visited June 28, 2021).

149. GDPR, *supra* note 8, art. 3.

150. GDPR, *supra* note 8, recital 142.

more than just standard practice . . . .The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data."[151] Though the GDPR no longer formally applies in the UK, the UK has its own data privacy protection law that has incorporated the GDPR provisions discussed here into a UK-specific law.[152] Thus, they continue to follow a similar data-protection focused model that can provide clarity in employment matters involving AI.

The consent requirement is different in the context of an employee, however.[153] The UK Information Commissioner has "issued guidance saying that the nature of the relationship between an employer and employee raises the question of how free[ly] this consent can be given."[154] In its Federal Data Protection Act, the German legislature defined consent as "freely given if it is associated with a legal or economic advantage for the employee or if the employer and employee are pursuing the same interest."[155] Additionally, this language imposes no requirement that the employee be a resident or citizen of the EU, meaning that the GDPR applies to any company that has employees present in the EU.[156] This applies to "employee data", which includes an employee's application, personnel file, payroll information, and any other information an employer may possess regarding their employees[157]. The GDPR effectively protects employees as data subjects of their employers with a consent requirement, a specific provision for "sensitive" data, a data protection impact assessment requirement, and notification of rights requirements.[158] While most data-based employee rights also existed under the Data Protection Directive that the GDPR intended to update, a new key factor under the

151. *Lawful Basis for Processing*, *supra* note 148.

152. *Information Rights After the End of the Transition Period – Frequently Asked Questions*, U.K. INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/transition-period-faqs/#gdpr (last visited June 28, 2021).

153. *See* PrivSec Report, *How Will GDPR Affect Employee Data*?, GRC WORLD FORUMS (May 29, 2018), https://gdpr.report/news/2018/05/29/how-will-gdpr-affect-employee-data/ ("When an EU citizen is an employee, then consent is no longer central.").

154. *Id.*

155. *Id.*

156. Sara H. Jodka, *The GDPR Covers Employee/HR Data and It's Tricky, Tricky (Tricky) Tricky*, DICKINSON WRIGHT (Apr. 2018), https://www.dickinson-wright.com/news-alerts/the-gdpr-covers-employee-hr-data-and-tricky.

157. *Id.*

158. *Id.*

GDPR is that an employee's "consent has to be freely given."[159] Additionally, when an employer takes the avenue of consent as a basis for data processing, employees also have the right to revoke that consent at any time.[160]

Enforcement

The greatest strength of the GDPR over the American AI Initiative is not only that it establishes strong legal levers for employees, as data subjects, but has rigidly enforced the standards that it has put in place.[161] One year after the GDPR entered force, the UK's Information Commissioner's Office imposed a hefty €22 million fine on British Airways for a breach of customer data.[162] Google has been fined €50 million, or nearly USD $57 million, "for not properly disclosing to users how data is collected across its services . . . to present personalized advertisements."[163] Just over six months after the GDPR took force, Germany's Regional Labour Court of Stuttgart considered a data subject's access rights under GDPR in "the context of compliance and whistle-blowing regimes."[164] Ultimately, the court held that "an employer was required not only to provide an employee with the records containing performance and behavioral data, but also to disclose information regarding internal investigations."[165] This ruling is in line rulings in the UK and Ireland, where data subject requests are often a mechanism used by employees to prepare for litigation.[166]

V. RECOMMENDATION

The GDPR was a small leap for the European Union, but a giant leap for mankind as some of the strongest and widest-

159. PrivSec Report, *supra* note 153.

160. *Lawful Basis for Processing*, *supra* note 148.

161. *See generally GDPR Enforcement Tracker*, CMS, https://www.enforcementtracker.com (last visited Jan. 24, 2020) (compiling fines and penalties that have been issued due to violations of the GDPR).

162. *Id.*

163. Satariano, *supra* note 61.

164. Cristoph Ritzer et al., *German Court Ruled That Protection of the Whistle-Blower Confidentiality Does Not Generally Override the Data Subject Access Right*, NORTON ROSE FULBRIGHT BLOG NETWORK (Mar. 22, 2019), https://www.dataprotectionreport.com/2019/03/german-court-ruled-that-protection-of-the-whistle-blower-confidentiality-does-not-generally-override-the-data-subject-access-right/.

165. *Id.*

166. *Id.*

sweeping data privacy regulations in the world. Perhaps the U.S. government is unwilling to regulate the tech industry because they do not want to step on the toes of the valuable tech firms.[167] Others have suggested that the government is hesitant to regulate the tech industry due to competition from large Chinese firms that are also rich with data.[168] Ready or not, however, the GDPR imposed a lot of the types of regulations the U.S. was so hesitant to impose on American tech firms. However clunky, a law based on the principles of transparency and fairness governing data disclosures was necessary to address the nature of harm in the an increasingly tech-dependent world, and create principles that guide how existing legal frameworks, like discrimination claims in employment, can remain effective with the proliferation of access to such technology.[169] On a larger scale, the U.S. will need to work with international allies in order to create sustainable, global standards that address transparency and fairness concerns while giving technology firms the legal protection and latitude to innovate.

Until a more comprehensive data privacy regulation is created and an enforcement agency is established, legal scholars, jurists and businesses should focus on the principles of the GDPR to guide their analysis of employment claims.[170] Expert administrative law professor Cary Coglianese has considered the impact of the black box problem that arises from algorithmic decision making on legal analysis, specifically the reasoning requirement of the Administrative Procedure Act.[171] The APA imposes certain due process and notice and explanation requirements on agencies, with varying levels of "reasoning" explanations required, pushing them to provide reasoned justifications for their actions.[172] Coglianese argues that officials would be able to "quite easily satisfy reasoned transparency"

167. *See* Alexis C. Madrigal, *Silicon Valley Abandons the Culture That Made It the Envy of the World*, ATLANTIC (Jan. 15, 2020), https://www.theatlantic.com/technology/archive/2020/01/why-silicon-valley-and-big-tech-dont-innovate-anymore/604969/.

168. *Id.*

169. *See* Raghavan et al., *supra* note 92, at 17 (summarizing the harms of unchecked use of data and AI).

170. *See generally* Cary Coglianese & David Lehr, *Transparency and Algorithmic Governance*, 71 ADMIN. L. REV. 1 (2019) (arguing that officials can use AI responsibly while not disclosing the full extent of their "black box" algorithms).

171. *Id.* at 20, 24–25.

172. *Id.* at 24–25.

because they could explain factors for consideration by providing a high-level description of how an algorithm functions.[173] Private companies, however, do not have the same disclosure requirements that the Freedom of Information Act imposes on government agencies.[174] Specifically in the employment discrimination context, where employers must articulate a non-discriminatory reason for an adverse action, lack of transparency requirements could leave employers without a non-discriminatory reason to shift the burden back to employees.

The "right to explanation" component of the GDPR has been the subject of many discussions.[175] Scholars have identified a number of legal and technical barriers to this right to explanation, including the technical challenge of understanding algorithmic rationale.[176] "Explanations can serve many purposes. To investigate the potential scope of explanations, it seems reasonable to start from the perspective of the data subject, which is the natural person whose data is being collected and evaluated."[177] Sandra Wachter and her colleagues have proposed three aims for explanations to assist the subjects of data collection practices: "(1) to inform and help the subject understand why a particular decision was reached (2) to provide grounds to contest adverse decisions, and (3) to understand what could be changed to receive a desired result in the future[.]"[178] They argued that the data handler should give "unconditional counterfactual explanations . . . for positive and negative automated decisions, regardless of whether the decisions are solely automated or produce legal or other significant effects."[179] Counterfactual explanations are advantageous because they bypass the technical black box problem, providing the data subject with information that is easily digestible without attempting to open the black box.[180] "The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the

173. *Id*. at 32.

174. *Id*. at 20 (explaining that FOIA requires government agencies to provide government documents to the public, but not private organizations).

175. Sandra Wachter et al., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR*, 31 HARV. J. L. & TECH. 841, 842 (2018).

176. *Id*. at 842–43.

177. *Id*. at 843.

178. *Id*.

179. *Id*. at 844.

180. *Id*. at 860.

algorithms used[.]"[181] This method encourages an honest exchange between employers and employees about algorithms, the data they processed and outcomes of that data, as opposed to requiring an entire deconstruction of exceedingly complex algorithmic black boxes.

Thus, until a data privacy regulation is passed at the federal level, or an agency is created to give more specific guidance to jurists and legal scholars, it would be helpful to focus on explanations of *how* the algorithmic learning was used in the decision-making process. This would allow plaintiff employees to better understand the process that generated their adverse action, while employers can reasonably explain results through counterfactuals, as opposed to attempting the daunting and seemingly impossible task of identifying exactly *why* the AI did what it did. This would allow companies that aim to protect their code as intellectual property to keep their "recipes" secret, while increasing transparency and accountability dialogue between employers and employees.

Additionally, state-level legislation regulating data privacy could also become more common until more robust federal-level legislation is enacted. California enacted a first-of-its-kind data privacy law that went into effect in early 2020: the California Consumer Privacy Act ("CCPA").[182] The CCPA is the toughest data privacy law in the United States and is anticipated to set the standard for national data privacy.[183] In addition to giving consumers greater ownership, control and security over their personal information, the CCPA "bestow[ed] two landmark rights on California employees, applicants, contractors, emergency contacts, and dependents: (1) the right to notice about what personal information an employer collects and the purpose of collection; and (2) the right to sue with statutory damages if sensitive data is compromised."[184] While the CCPA was largely based on the GDPR, it is "notably less extensive and

181. *Id.* at 867.

182. CAL. CIV. CODE § 1798.100 (West 2020); Rachel Myrow, *California Rings in the New Year With a New Data Privacy Law*, NAT'L PUB. RADIO (Dec. 30, 2019, 9:00 AM), https://www.npr.org/2019/12/30/791190150/california-rings-in-the-new-year-with-a-new-data-privacy-law.

183. *Id.*

184. Justine M. Phillips & Alexandra M. Gross, *The Heart of Employee Rights Under CCPA: Attorney General Modifies Guidance*, NAT'L L. REV. (Feb. 14, 2020), https://www.natlawreview.com/article/heart-employee-rights-under-ccpa-attorney-general-modifies-guidance.

less stringent than its EU predecessor[.]"[185] Despite being nicknamed "GDPR Lite", the CCPA shares the GDPR's emphasis on transparency, and creates an unprecedented consumer right to bring action against companies that violate their rights under the CCPA.[186] In doing so, the CCPA not only creates greater rights for employees, but also creates greater awareness surrounding the transparency issues that might arise from the black box problem for business. At minimum, employees and applicants in California[187] now have a legal right to know what data is being collected and emphasizing *how* it is being used. While it is too soon to tell whether the CCPA will make it easier to evaluate employment claims that involve AI, creating employee rights in the data about them is definitely a step in the right direction.

VI. CONCLUSION

In an interesting "Ideas" piece from *The Atlantic*, executives at Microsoft, including the company's President, wrote an important piece with a surprising call for more regulation over the tech industry:

> Information technology is having an immensely uneven economic impact on the world, creating huge wealth for some while leaving others behind, as it displaces jobs and fails to reach communities that lack broadband connectivity. It's changing the face of war and peace, creating a new theater of warfare in cyberspace and new threats to democracy through state-sponsored attacks and disinformation. And it's increasing the polarization of domestic communities, eroding privacy, and creating an emerging capability for authoritarian regimes to exercise unprecedented surveillance of their citizens. As artificial intelligence continues to advance, all these developments will accelerate.[188]

---

185. KJ Dearie, *Comparing the CCPA and the GDPR*, CPO MAGAZINE (Mar. 26, 2020), https://www.cpomagazine.com/data-protection/comparing-the-ccpa-and-the-gdpr/.

186. *Id.*

187. *See* Michelle A. Schaap, *Not in California? Here's Why the CCPA Should Still Be on Your Radar*, CHIESA SHAHINIAN & GIANTOMASI PC (Nov. 2019), https://www.csglaw.com/not-in-california-heres-why-the-ccpa-should-still-be-on-your-radar (postulating that the CCPA, like the GDPR, is structured to extend regulations to for-profit businesses that meet certain criteria, even if they are not based in California).

188. Smith & Browne, *supra* note 68.

While the U.S. has taken small steps to address the internet and data revolutions, the policy lacks the emphasis on transparency and enforcement mechanisms that make Europe the "world's most aggressive tech watchdog".[189] A lack of transparency, especially the "black box" problem, will exacerbate existing issues for employee-plaintiffs by making it more difficult to establish the statistical disparities that can be the basis of a disparate impact discrimination case. Employers are not immune from the effects of this technology, since explaining business reasoning becomes difficult for decisions based on algorithms not fully understood by employers. Europe and similarly data protection-focused countries like the U.K. are equipped with GDPR models emphasizing data subject rights, fairness and transparency. The U.S., on the other hand, has not enumerated any such rights on the federal level, nor has it given meaningful guidance to the private sector on AI best practices. The current system for evaluating disparate impact claims will leave both employees and employers at a significant disadvantage with the introduction of algorithms to the decision-making process in human resources. With its emphasis on transparency and strong enforcement mechanisms, the GDPR has created a framework of data privacy rights that creates rights of access for employees and structural requirements for companies that guide ethical and thoughtful uses of AI. Until the U.S. is able to create a cohesive, national tech policy, employers and developers of people analytics tools should consider using GDPR principles, especially transparency and fairness, while developing and using of AI-based technologies.

189. Satariano, *supra* note 61.