NOTE

PEOPLE ANALYTICS AND INDIVIDUAL AUTONOMY: EMPLOYING PREDICTIVE ALGORITHMS AS OMNISCIENT GATEKEEPERS IN THE DIGITAL AGE WORKPLACE

Erica Pedersen*

People Analytics is a powerful tool with immense promise for enhancing organizational insights. However, this Note argues that employers' unfettered use of opaque predictive algorithms, which are trained on behavioral data to profile workers and guide employment outcomes, represents a significant threat to individual autonomy. Part II explores the emergence of People Analytics as a continuation and merger of historical approaches to scientific management in the American workplace. Part III contrasts the organizational benefits of predictive analytics against the uniquely intrusive, non-transparent, and sometimes arbitrary manner in which they are currently deployed against workers. Part IV discusses how People Analytics may hasten the erosion of employees' normative rights in the workplace. It then discusses the insufficiency of existing regulatory and common law mechanisms to protect workers from arbitrary or discriminatory decisionmaking based on algorithmic profiling. Finally, Part V reviews some proposed solutions, emphasizing the importance of employee voice and the need for proactive regulations to enforce algorithmic transparency and protect individuals' rights to privacy and autonomy.

I.   INTRODUCTION

Every day, big data analytics play a powerful and often decisive role in determining the choices and opportunities available to individuals. Opaque, privately-developed

algorithms control access to credit and loans,[1] guide policing and criminal sentencing decisions,[2] segment insurance markets,[3] and target delivery of news, services, and advertising,[4] among many other applications.[5] To achieve these goals, companies increasingly rely on artificial intelligence (AI) to rank and predict individuals' personal preferences, purchasing behavior, financial intelligence, political attitudes, movements, and health.[6] Despite the huge impact that experts predict big data analytics will have on society in the future,[7] many individuals remain unaware of the full extent to which pervasive algorithmic profiling already guides or constrains their actions.[8] Algorithms receive trade secrets protection,[9] which can facilitate the rapid

---

[1] *See* Vlad A. Hertza, Note, *Fighting Unfair Classifications in Credit Reporting: Should the United States Adopt GDPR-Inspired Rights in Regulating Consumer Credit?*, 93 N.Y.U. L. REV. 1707, 1709–11 (2018); Shaun B. Spencer, *Privacy and Predictive Analytics in E-Commerce*, 49 NEW ENG. L. REV. 629, 637–38 (2015).

[2] *See* Ric Simmons, *Big Data, Machine Judges, and the Legitimacy of the Criminal Justice System*, 52 U.C. DAVIS L. REV. 1067, 1069–70 (2018); Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109, 1112–15 (2017).

[3] *See* Bernard Marr, *How AI and Machine Learning Are Used To Transform the Insurance Industry*, FORBES (Oct. 24, 2017, 12:28 AM), https://www.forbes.com/sites/bernardmarr/2017/10/24/how-ai-and-machine-learning-are-used-to-transform-the-insurance-industry/#6e080cb713a1 [https://perma.cc/WH5G-VS2U].

[4] *See* Spencer, *supra* note 1, at 634–35 (discussing predictive models used for advertising, including those that draw on information from news and service providers).

[5] *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 2–3 (2014).

[6] *See id.* at 3–4.

[7] *See* LEE RAINIE & JANNA ANDERSON, PEW RSCH. CTR., CODE-DEPENDENT: PROS AND CONS OF THE ALGORITHM AGE 3–5 (2017), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/02/PI_2017.02.08_Algorithms_FINAL.pdf [https://perma.cc/J9DR-658U].

[8] *Id.* at 7.

[9] *Cf.* Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 121–25 (2019) (discussing trade secrets protections for algorithms).

development and monetization of new applications for predictive analytics. But the consequent lack of transparency has also impeded efforts to verify the integrity of algorithmic construction, the robustness of algorithmic results, and the social and ethical implications of deploying such methods to make life-altering decisions at scale.[10]

In the employment context, People Analytics[11] algorithms can guide and automate decisions throughout the human resources life cycle, including recruitment, hiring, performance assessment, promotion, compensation, and benefits management decisions.[12] These algorithms combine traditional employment data with "nontraditional" data derived from sources far beyond the workplace, collected internally or purchased from data brokers.[13] The algorithm identifies correlations in the data set and generates profiles expected to predict the future behavior and performance of workers with shared characteristics.[14] These algorithmic insights are extraordinarily wide-reaching, covering individuals' behavior, personalities, habits, health, state of mind, social proclivities, and any other metrics that the coders

---

[10] *See, e.g.*, *id.* at 123–24, 126–27.

[11] People Analytics is a human resources management practice "concerned with the use of information technologies, descriptive and predictive data analytics and visualization tools for generating actionable insights about workforce dynamics, human capital, and individual and team performance that can be used strategically to optimize organisational effectiveness, efficiency and outcomes, and improve employee experience." Aizhan Tursunbayeva et al., *People Analytics—a Scoping Review of Conceptual Boundaries and Value Propositions*, 43 INT'L J. INFO. MGMT. 224, 231 (2018) (emphasis deleted). Related terms include HR Analytics, Human Capital Analytics, Talent Analytics, and Workforce Analytics. *Id.* at 226.

[12] *See* Rebecca J. Wilson et al., *Busting the Black Box: Big Data, Employment and Privacy*, DEF. COUNS. J., July 2017, at 1, 8.

[13] Sources of nontraditional employment data include "public records, social media activity logs, sensors, geographic systems, internet browsing history, consumer data-tracking systems, [and] mobile devices," among many others. *See id.*

[14] *See* Robert Sprague, *Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics*, 21 RICH. J.L. & TECH., Apr. 24, 2015, at 31–33.

or the AI has determined are statistically relevant to labor productivity.[15]

Since its emergence in the early 2000s, the field of People Analytics has developed rapidly in the United States.[16] A 2017 Deloitte study found that seventy-one percent of companies view People Analytics as a "high priority" in their organizations and noted "explosive growth" in the use of "interaction analytics (studying employee behavior) to better understand opportunities for business improvement."[17] Despite the widespread interest in People Analytics technologies, a recent scoping review noted "little evidence of the benefits promised" by People Analytics vendors and warned that additional research is necessary to determine whether their methods in fact generate "measurable organizational impacts."[18] While People Analytics' mass collection and analysis of data is useful for identifying correlations,[19] controlled experimentation is necessary to obtain a more robust understanding of causality.[20]

---

[15] *See infra* Section III.C.

[16] *See* Janet H. Marler & John W. Boudreau, *An Evidence-Based Review of HR Analytics*, 28 INT'L J. HUM. RES. MGMT. 3, 6, 18, 23–24 (2017) (observing increased interest in People Analytics but also noting lags in implementation and scholarly scientific research).

[17] *See* David R. Fineman, *People Analytics: Recalculating the Route*, DELOITTE (Feb. 28, 2017),

https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2017/people-analytics-in-hr.html   [https://perma.cc/SFK7-KK8M] (summarizing the study).

[18] *See* Tursunbayeva et al., *supra* note 11, at 230. This 2018 study also noted "a marked absence of ethical considerations" in the literature discussing People Analytics practices and found that the authors of most published articles on People Analytics "came from consulting or technology companies." *Id.* at 230–32.

[19] *See* Steve Lohr, *Scientific Management Redux: The Difference Is in the Data*, N.Y. TIMES: BITS (Apr. 21, 2013, 11:29 AM), https://bits.blogs.nytimes.com/2013/04/21/scientific-management-redux-the-difference-is-in-the-data/?action=click&module=RelatedCoverage&pgtype=Article&region=Footer [https://perma.cc/Z786-4HVV].

[20] *See id.* Former FTC Chairwoman Edith Ramirez has warned that predictive correlations "may feel like arbitrariness-by-algorithm" for

There are growing public policy concerns surrounding the largely unregulated use of big data analytics to control employment opportunities. Data aggregation practices and predictive algorithms pose a clear threat to employee privacy and autonomy.[21] There is also substantial evidence that the outputs of these methods can be arbitrary and insidiously discriminatory: People Analytics algorithms may reproduce existing structural inequalities in the workplace,[22] make decisions based on seemingly neutral factor, which function as proxies for protected characteristics,[23] and infer sensitive health-related information about employees.[24] The lack of transparency in the construction and application of People Analytics algorithms may undermine employee and public confidence, resulting in tensions which could skew data and

mischaracterized individuals. Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from the Lifeguard's Chair 7–8 (Aug. 19, 2013),
https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf [https://perma.cc/J9TT-FBVT] (remarks as prepared).

[21] *See* Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 Fordham Intell. Prop. Media & Ent. L.J. 803, 806, 809–10 (2017); Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 94 (2014).

[22] *See* Miriam A. Cherry, *People Analytics and Invisible Labor*, 61 ST. LOUIS U. L.J. 1, 12–14 (2016); Jordan Weissmann, *Amazon Created a Hiring Tool Using A.I. It Immediately Started Discriminating Against Women.*, SLATE (Oct. 10, 2018, 4:52 PM), https://slate.com/business/2018/10/amazon-artificial-intelligence-hiring-discrimination-women.html [https://perma.cc/5ALL-W4T4].

[23] *See* Pauline T. Kim & Sharion Scott, *Discrimination in Online Employment Recruiting*, 63 ST. LOUIS U. L.J. 93, 98 (2018); Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 880 (2017).

[24] *See* Valentina Zayra, *Employers Are Quietly Using Big Data to Track Employee Pregnancies*, FORTUNE (Feb. 17, 2016, 5:36 PM), http://fortune.com/2016/02/17/castlight-pregnancy-data/ (on file with the Columbia Business Law Review) (discussing inferences about, inter alia, pregnancy and diabetes).

cut against the productivity benefits offered by the system.[25] Anecdotal accounts suggest that the replacement of management with AI has already engendered some backlash from job applicants.[26] More broadly, following an onslaught of data breaches at large technology companies, there is a crisis in consumer trust, as well as heightened public awareness of the importance of data privacy.[27]

Predictive algorithms can be incredibly useful sources of organizational knowledge. But the design and deployment of algorithms to make predictions about individual workers for the benefit of an institution or company implicates fundamental human rights. As one scholar has noted, "today's workers are left with a Hobson's choice of giving up their privacy or giving up their job, if the predictive analytics even allow them to have the job."[28] To preserve the enormous potential value of algorithmic insights, transparency is key. Focusing on the growing application of People Analytics as a gatekeeping mechanism in the workplace, this Note contends that data privacy laws aimed solely at regulating the collection of and access to personal data[29] will not deter the most fundamental threats that these methods pose to individual autonomy.

---

[25] *Infra* Section III.B.

[26] *See* Nick Corcodilos, *HireVue Video Interviews: HR Insults Talent in a Talent Shortage*, ASK THE HEADHUNTER (Aug. 22, 2016), https://www.asktheheadhunter.com/9044/hirevue-video-interviews-insult-talent-in-talent-shortage [https://perma.cc/8RHQ-ER8U] (noting objections to an automated interview system).

[27] *Cf.* BROOKE AUXIER ET AL., PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 2, 4 (2019), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf [https://perma.cc/RJ8P-AS6N] (finding significant public concern about companies' collection and "steward[ship]" of data).

[28] Sprague, *supra* note 14, at 46 (footnotes omitted).

[29] *See, e.g.*, California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–.199 (2020).

The pervasive automation of employment decisions based on opaque algorithmic presumptions implicates human rights on a societal level. In controlling access to job opportunities, these systems will impact the structure and trajectory of society as a whole.[30] Should private developers and employers hold this degree of social power? What assumptions may an algorithm make about a person based on a behavioral profile? What opportunities may it offer or withhold based on those assumptions? What will be the broader social impact of relinquishing decisions to opaque algorithmic arbiters coded by for-profit companies? To preserve individuals' normative rights to autonomy, privacy, and due process, we must regulate the use of personal and behavioral data to develop tools that may arbitrarily and discriminatorily reshape workers' lives.

This Note argues that employers' unfettered use of predictive algorithms trained on behavioral data to make inferences about individual employees represents a significant threat to employee autonomy. Part II provides a brief overview of the evolution of scientific management in the American workplace and the emergence of People Analytics as a foreseeable outcome of decades of research into labor productivity maximization, behavioral psychology, and data science. Part III delves into the application of People Analytics systems to highlight how employers increasingly subject American workers to statistical profiling in a manner that is uniquely intrusive, non-transparent, and arbitrary. Part IV discusses the ways in which People Analytics may hasten the erosion of employees' normative rights in the workplace and the insufficiency of existing regulatory and common law mechanisms to protect employees from potentially arbitrary or discriminatory decisionmaking based on algorithmic profiling. Finally, Part V reviews some proposed solutions, emphasizing the importance of employee voice and the need for proactive regulations to enforce transparency and preserve individuals' dignity and autonomy in the workplace.

---

[30] *See supra* note 7, at 20–21.

II.   PEOPLE ANALYTICS: SCIENTIFIC MANAGEMENT FOR THE DIGITAL AGE

People Analytics is essentially the modern incarnation of data-based employee productivity maximization.[31] Given the United States's history of managerial paternalism, it is no surprise that the development of analytical methods for big data has resulted in the emergence of a new brand of workforce science fueled by digital technologies and surveillance of workers.

A. Managerial Paternalism and Historical Efforts to Maximize Labor Productivity

Managers have long viewed a company's ability to understand and incentivize effectively its workforce as a key driver of success. Early industrial management techniques reflected an understanding of workers' as individuals in a social environment, not simply as inputs in the production process.[32] The scope of managerial intervention for the sake of labor productivity covered workers professional and personal activities. Company town bosses "used their power as owners of the village to control their employees" outside of the workplace.[33] Workers were disciplined for trivialities such as "failing to maintain their homes and yards in good condition."[34]   Henry   Ford's   Sociological   Department investigated and managed employees' private lifestyles,

---

[31] This Note focuses on the types of People Analytics services that employ algorithms to provide predictive and prescriptive outputs designed to guide or control an end user's decisions. However, the term People Analytics may also describe technologies which offer purely descriptive visualizations of business metrics in real time, relying on humans to analyze and manipulate these data. Those non-predictive algorithms are outside the scope of this Note.

[32] *See id.*

[33] *See* M. Todd Henderson, *The Nanny Corporation*, 76 U. Chi. L. Rev. 1517, 1536 (2009) (internal quotation marks omitted) (quoting Margaret Crawford, *Earle S. Draper and the Company Town in the American South*, *in* The Company Town: Architecture and Society in the Early Industrial Age 139, 144 (John S. Garner ed. 1992)).

[34] *See* Henderson, *supra* note 33, at 1537.

including their health and personal vices, to enhance employee productivity.[35] Managers could and did monitor workers to police perceived moral failings, despite the dubious connections between such oversight and organizational efficiency.[36]

Around the turn of the twentieth century, as industrial operations grew rapidly in both scale and complexity, Taylorism emerged, promoting labor productivity maximization through meticulous recording, analyzing, and recalibrating of workers' actions.[37] At the root of this strategy was the novel concept of "scientific management," which involved "breaking down workplace tasks into their smallest possible units and then creating rigorous protocols for these task units to maximize efficiency."[38] Employees in this era became "components to be stratified, incentivised, deployed and shed for maximum effectiveness."[39] Yet, as one article points out, Taylorism's "failure to recognize the importance of the individual worker" led to a reaction placing greater weight on "the needs and wants" of employees.[40] Ultimately, new personnel management strategies ousted Taylorism and originated the field of human resources.[41]

These invasive management techniques also engendered significant backlash and anxiety within the workforce. The workers' movement advocated for standardized working hours to "safeguard[] workers' non-work time from the demands of employers" and "ensure that workers would have sufficient leisure time to dedicate to self-development and political

---

[35] *See* Bodie et al., *supra* note 37, at 966. Ford ultimately disbanded the Sociological Department, in part because he believed "[w]elfare work that consists in prying into employees' private concerns is out of date." *See id.* (quoting HENRY FORD, MY LIFE AND WORK 130 (Doubleday, Page & Co. 1922)).

[36] *See* Henderson, *supra* note 33, at 1537.

[37] *See* Matthew T. Bodie et al., *The Law and Policy of People Analytics*, 88 U. COLO. L. REV. 961, 965 (2017).

[38] *Id.*

[39] *See* Tursunbayeva et al., *supra* note 11, at 224.

[40] *See* Bodie et al., *supra* note 37, at 965–66.

[41] *See id.* at 965.

participation as citizens."[42] As a compromise, both the Fair Labor Standards Act of 1938 (FLSA) and the National Labor Relations Act of 1935 (NLRA) articulated a formal distinction between work and nonwork times and spaces.[43] For a few decades, this dichotomy provided some protection against employer intrusion into and control over employees' private lives and organizing activities.[44]

But during World War I and particularly after World War II, the advent of psychology-based personality, intelligence, and aptitude tests revolutionized the field of personnel management.[45] The rich data sets produced as a result of the Army's analysis of the abilities and personalities of soldiers were repurposed to develop assessments for employees' managerial and professional capabilities.[46] Although some employers still use versions of these aptitude tests to screen applicants, their popularity waned significantly in the 1970s due to widespread worker resistance, efficacy concerns, and enhanced liability exposure under anti-discrimination laws.[47]

Over the last few decades, rapid developments in digital technologies and data processing have opened the door to an even more powerful and omniscient form of managerial paternalism: People Analytics.[48] Employers are now able to collect and analyze massive amounts of observational and behavioral data from workers' personal and professional activities, then operationalize the resulting inferences and predictions to maximize organizational profits.[49] People Analytics initiatives combine Taylorism's workers-as-inputs mindset with Fordism's pervasive intrusion into employees personal lives, and wield this data to algorithmically

---

[42] Shirley Lung, *Overwork and Overtime*, 39 IND. L. REV. 51, 57 (2005).

[43] *See* Leora Eisenstadt, *Data Analytics and the Erosion of the Work/Nonwork Divide*, 56 AM. BUS. L.J. 445, 450–54.

[44] *See id.* at 450–54, 465.

[45] *See* Bodie et al., *supra* note 37, at 966–67.

[46] *See id.* at 967.

[47] *See* Lohr, *supra* note 19.

[48] *See supra* notes 15–17 and accompanying text.

[49] *See supra* notes 11–14 and accompanying text.

maximize organizational profit.[50] These algorithms also rely on statistical correlations that may reintroduce arbitrary and discriminatory inaccuracies similar to those found in intelligence and aptitude tests,[51] albeit in a more opaque and less accountable manner.[52] But before analyzing the novel (and familiar) threats that algorithmic profiling poses to workers' rights, it is helpful to understand the technology underlying People Analytics systems.

B. Constructing People Analytics Algorithms

Predictive algorithms rely on statistical models based on well-defined methodologies for cleansing, preparing, and evaluating data, as well as methodologies for evaluating the effectiveness of the model itself.[53] Although scholars describe the process in a number of ways, broadly speaking there are five stages to predictive analytics: "data collection, data preparation, data mining, interpretation, and [action based on] the discovered knowledge."[54]

1. Data Preparation

"Data preparation involves rearranging and ordering the data, which sometimes involves aggregating very granular information into bigger categories."[55] Employers collect detailed data from employees or data brokers for myriad reasons, which are often unrelated to their subsequent uses of the same data.[56] There are few legal restrictions on the collection and sale of anonymized data derived from individuals' digital footprints, despite that analysts can often

---

[50] *See* Rainie & Anderson, *supra* note 7, at 42–43.

[51] *See* U.S. EQUAL EMP'T OPPORTUNITY COMM'N, EEOC-NVTA-2007-2, EMPLOYMENT TESTS AND SELECTION PROCEDURES (2007).

[52] *See supra* notes 21–26 and accompanying text.

[53] *Cf.* JAMES WU & STEPHEN COGGESHALL, FOUNDATIONS OF PREDICTIVE ANALYTICS 1–4 (Vipin Kumar ed., 2012) (summarizing the basics of statistical modeling).

[54] *See* Bodie et al., *supra* note 37, at 969.

[55] *Id.* at 970.

[56] *See id.* at 969–70.

trace this "anonymous" data to their individual sources and that algorithms may be capable of predicting personally identifiable information based on aggregated anonymized data.[57] Employers also gather data internally from monitoring technologies embedded in company-owned hardware, employees' cell phones, and wearable technologies given to employees.[58] "If the data is legally obtained, it can generally be analyzed however the employer sees fit."[59]

Scholars warn that the psychological effects that pervasive surveillance has on workers may skew the data, because the effects may cause discomfort leading to less favorable measurements.[60] Moreover, there is reason to be concerned about the quality and accuracy of the data collected.[61] For example, some employers use biometric data from trackers like the Fitbit, but Fitbit has faced numerous lawsuits alleging that its wearable biometric trackers are systematically inaccurate.[62]

2. Designing Algorithms

The importance of data accuracy becomes evident during the next steps in the algorithmic process: data mining and interpretation. Data mining involves an automated statistical analysis of the database to find new patterns or fit data within

---

[57] *See* Crawford & Schultz, *supra* note 21, at 96–99 (discussing the acquisition and use of data).

[58] *See* Pauline T. Kim, *Data Mining and the Challenges of Protecting Employee Privacy Under U.S. Law*, 40 COMPAR. LAB. L. & POL'Y J. 405, 405–06 (2019).

[59] Bodie et al., *supra* note 37, at 999.

[60] *See* Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS U. L.J. 21, 52 (2018) (discussing this issue with an emphasis on wearable technology).

[61] *See* Bodie et al., *supra* note 37, at 1001.

[62] *See* Jason Bloomberg, *From Fitbit to Volkswagen: The Dangers of Inaccurate Data*, FORBES (Jan. 10, 2016, 10:28 PM), https://www.forbes.com/sites/jasonbloomberg/2016/01/10/from-fitbit-to-volkswagen-the-dangers-of-inaccurate-data/#527a0031653d [https://perma.cc/B83N-3WAA] (discussing accuracy issues); Ajunwa, *supra* note 54, at 47 (discussing employers' use of the Fitbit).

known patterns.[63] No statistical model is perfect and each involves unique tradeoffs, so employers choose models based on available data and current business objectives.[64] As reality diverges from the assumptions underlying those models, however, the accuracy of their analyses may decline.[65] The key issue "is that no one knows what the predictive outcome will be and whether that prediction will be valid the next day or the one after that."[66] Moreover, correction may be difficult. Models usually detect correlations among diverse data from incredibly varied sources, so their predictions will be "founded on informational attributes that are increasingly random and unintuitive to both the employee and the employer."[67] Large data sets are especially vulnerable "to generating . . . false or spurious statistical relationships. . . . because the risk of an algorithm surfacing a statistically significant but contextually meaningless connection between variables increases as the size of the data sets increases."[68] Thus, it is necessary to understand the assumptions underlying a model and to test and improve the model continually to ensure that its outputs do not tend towards arbitrariness or irrelevance. This verification requires algorithmic transparency.[69]

When a programmer designs an algorithm, they must identify the variables the algorithm will use as inputs and the

---

[63] *See* Bart W. Schermer, *The Limits of Privacy in Automated Profiling and Data Mining*, 27 COMPUT. L. & SEC. REV. 45, 46 (2011).

[64] *Cf.* WU & COGGESHALL, *supra* note 53, at 1–3 (discussing the model-building process).

[65] *See id.* at 4–5.

[66] Mark Burdon & Paul Harpur, *Re-Conceptualising Privacy and Discrimination in an Age of Talent Analytics*, 37 UNIV. NEW S. WALES L.J. 679, 701 (2014).

[67] *See id.* at 692.

[68] Sarah   Valentine,   *Impoverished   Algorithms: Misguided Governments, Flawed Technologies, and Social Control*, 46 FORDHAM URB. L.J. 364, 389 (2019).

[69] *See* Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1239 (2017) (noting monitoring and other issues related to a lack of algorithmic transparency).

output variables it will "target."[70] The predictive targets of People Analytics systems are often, at least in part, qualities believed to be necessary for a "good" or "productive" employee.[71] Some of the most popular targets include measures of employees' values, cultural fit, and engagement.[72] Such measures are inherently subjective. Thus, human biases will inevitably infect the algorithm.[73] The complex relationship between values and the treatment of data also require that the programmers possess deep understandings of the contexts in which the algorithms will operate. But especially given the proliferation of third-party People Analytics vendors, this knowledge is typically absent among those developing the algorithm.[74]

The importance of heightened transparency is evident in the failures of the privately-developed "value added" algorithms used by numerous school districts around the country to predict teacher competency and guide termination decisions.[75] Teachers' unions led the effort to question these

[70] *See* Ignacio N. Cofone, *Algorithmic Discrimination Is an Information Problem*, 70 HASTINGS L.J. 1389, 1402 (2019).

[71] *See* Bodie et al., *supra* note 37, at 1018.

[72] *See* Tursunbayeva et al., *supra* note 11, at 230 (discussing the aims of People Analytics).

[73] *See* Cofone, *supra* note 70, at 1402.

[74] *See* Valentine, *supra* note 68, at 374 (discussing the unrepresentative population working in People Analytics).

[75] For a discussion of these algorithms and challenges to them, see Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM L. REV. 1265, 1280–83 (2020); *see also* Houston Fed'n of Tchrs., Loc. 2415 v. Houston Indep. Sch. Dist., 251 F. Supp. 3d 1168, 1177–80 (S.D. Tex. 2017). Plaintiffs' success in this matter ultimately depended on the testimonies of experts and the developer:

> During litigation, the school district could not explain the algorithm's outputs and refused to provide information about the algorithm itself, arguing that it did not have 'custody, control or possession' of the technology. The school district also admitted that it ceded all teacher evaluations to the algorithm's developer and did not verify or audit the scores the algorithm provided.

Valentine, *supra* note 68, at 373 (footnotes omitted) (quoting Houston Fed'n of Tchrs, 251 F. Supp. 3d. at 1177 n.28).

algorithms and force disclosures that laid bare errors embedded in their design.[76] Thus, one court found New York's value added teacher assessment system to be "arbitrary and capricious" in application.[77]

Algorithmic complexity and opacity present substantial obstacles to employees challenging algorithms' discriminatory or arbitrary uses. Trade secret protections significantly limit access to algorithms' underlying data and source codes, information that is integral to plaintiffs' ability to show discriminatory impact.[78] Moreover, even employers may be blind to algorithms' mechanics, either because third-party vendors developed the algorithms[79] or because machine learning algorithms may "independently update[] the variables or interactions [they] consider[] in reaction to the data [they] receive[]," making their reasoning unclear.[80]

3. Training Algorithms

After choosing a model, including input and target variables, a programmer trains their algorithm to make predictions using a set of "training data" assumed to "follow the same distribution as the data on which that model will have to work."[81] Any inaccuracies or misrepresentations in the training data will be baked into the model, heightening the potential for discriminatory or arbitrary results.[82] Moreover, by predicting the qualities of good future workers based on qualities of current and past workers, People

---

[76] *See* Bloch-Wehba, *supra* note 75, at 1281.

[77] Lederman v. King, 47 N.Y.S. 3d 838, 846–47 (N.Y. Sup. Ct. 2016).

[78] In *Muñoz v. Orr*, the Fifth Circuit declined to compel the Air Force to disclose its secret promotion algorithm because plaintiffs did not object in the court below and because denying access was not plain error. 200 F.3d 291, 305 (5th Cir. 2000). The court then dismissed the case on summary judgment because the plaintiff did not produce statistical evidence of disparate impact or treatment. *See id.* at 304.

[79] *See* Charlotte S. Alexander & Elizabeth Tippett, *The Hacking of Employment Law*, 82 MO. L. REV. 973, 998 (2017).

[80] *See id.*

[81] *See* Bodie et al., *supra* note 37, at 1016.

[82] *See id.*

Analytics algorithms "run[] the risk of homosocial reproduction, or replacement of workers with workers that look like them, on a grand scale."[83] If the training data only reflect a particular subset of the population, the algorithms' analyses and predictions generally will not be valid for other populations.[84] Thus, scholars warn that even well-designed algorithms will "replicate and amplify the preexisting biases and [structural] discrimination" present in society.[85]

4. Algorithms and Human Rights

Choices at each stage of the algorithm design process implicate fundamental human rights.[86] A focus on solutions tailored to particular stages of the algorithmic construction process risks ignoring some risks of People Analytics systems deployed at scale in workplaces throughout the country. Predictive algorithms, including People Analytics algorithms, threaten societal norms of freedom and autonomy by using statistical profiles to control access to opportunities, knowledge, and choice across many facets of life for entire populations.[87] Considering the vulnerabilities at each stage of the algorithm design process, it is evident that regulations which merely constrain access to certain data or mandate testing for discriminatory impact will not render predictive algorithms innocuous. Instead, a deeper conversation about acceptable uses and boundaries of algorithmic control is necessary to ensure that solutions are properly calibrated to the scale of the risks of that control. As we delegate more responsibilities to machine intelligence, we must take care to preserve norms of individual autonomy, privacy, and due process. Section III will discuss the present risks to these normative rights.

---

[83] *See id.* at 1013.

[84] *See id.* at 1016.

[85] *See* Valentine, *supra* note 68, at 383.

[86] For example, Pauline Kim has written numerous articles about the impact of discriminatory algorithms on employment. *See, e.g.*, *generally* Kim, *supra* note 23; Kim & Scott, *supra* note 23.

[87] *See* Balkin, *supra* note 69, at 1235–37.

III.   UNLEASHING PREDICTIVE ANALYTICS IN THE WORKPLACE

Like its predecessors in the field of workforce science, People Analytics promises new insights and cost savings associated with more efficient and calibrated methods of employee management.[88] In pursuit of these goals, People Analytics systems cast a wide net over employees' lives, aggregating and mining data collected from a broad range of sources, including wearable technologies,[89] smart phone applications, internet browsing history, and social media. [90] These systems try to measure the "true sources of [worker] productivity," track how employees stack up using these measures, then incentivize the most productive behaviors to enhance employees' future performance.[91]

A. The Business Case for People Analytics

Proponents of People Analytics argue that algorithmically guided or controlled decisionmaking will eliminate subjective bias in human resources management,[92] enhance accountability by offering reliable explanations for decisions,[93] and even help employees discover and signal their own talents and skills.[94] Yet the true economic value of People Analytics lies in the technology's ability to generate profit-maximizing predictions by parsing massive data sets for

---

[88] *See* Nathaniel M. Glasser, Frank C. Morris Jr. & Katherine Smith, *Big Data, People Analytics and Employment Decisions: The Rewards and Often-Overlooked Risks*, WESTLAW J. EMP., Mar. 27, 2018.

[89] *See* Ajunwa, *supra* note 60, at 34–42.

[90] *See* Wilson et al., *supra* note 12, at 8 (describing the variety of sources of data).

[91] *See* Bodie et al., *supra* note 37, at 969.

[92] *See* Kim, *supra* note 23, at 869.

[93] *See* Ed Felten, *Algorithms Can Be More Accountable than People*, FREEDOM TO TINKER (Mar. 19, 2014), https://freedom-to-tinker.com/2014/03/19/algorithms-can-be-more-accountable-than-people/ [https://perma.cc/89HL-6PFJ].

[94] *See* Bodie et al., *supra* note 37, at 978.

statistical correlations.[95] Beyond merely constructing a descriptive profile of the 'successful' or 'happy' employee, People Analytics algorithms make inferences to guide management. For instance, by predicting which behavioral profile a particular applicant or employee is statistically likely to fit, an algorithm can recommend or, if given enough autonomy, automatically implement a particular action with respect to that individual.[96]

People Analytics systems can identify previously obscure or counterintuitive correlations in data sets and use them to develop risk profiles related to organizational productivity.[97] "[I]nnovations in storage capacity, data aggregation techniques and cross-contextual linkability enable new forms of idiopathic predictions," a phenomenon that scholars refer to as "the computational turn."[98] Thus, these systems allow companies to evaluate whether traditionally-accepted or unexpected indicators of success better correlate with business outcomes. Ideally, this capability will drive beneficial innovation in hiring and talent management practices.

For instance, one People Analytics algorithm found that people with criminal backgrounds actually perform better as call center employees than those without such backgrounds.[99] Given the extraordinary difficulties that individuals with criminal records face in the employment market,[100] this algorithmic output could have the desirable effect of reducing discrimination against job applicants with criminal records by

---

[95] *Cf.* Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 67 (2013) (observing that many predictive algorithms have the prosaic aim of increasing sales).

[96] *See supra* notes 10–14 and accompanying text.

[97] *See* Burdon & Harpur, *supra* note 66, at 692.

[98] Ian Kerr, *Prediction, Preemption, Presumption: The Path of Law After the Computational Turn*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 91, 92 (Mireille Hildebrandt & Katja de Vries eds., 2013).

[99] *See Robot Recruiters*, ECONOMIST, Apr. 6, 2013, at 78, 78.

[100] *See id.* ("[F]irms routinely cull job candidates with a criminal record.").

reducing the perceived relevance of a criminal record to productivity. However, depending on the disposition of available data at a given moment, an algorithm may also suggest that employers attach enhanced relevance to highly subjective characteristics with an attenuated relationship to the employee's job duties. Evolv, a vendor of People Analytics software, helped Xerox construct a profile of the ideal customer-care representative and attached relevance to other characteristics based on complex correlations.[101] Its model favored employees who were "creative but not overly inquisitive," and who were members of at least "one but no more than four social networks."[102] The identification, interpretation, and operationalization of correlations like these fundamentally depends on the opinions embedded in the algorithm's code.

People Analytics systems also can synthesize quickly new data derived from real-time monitoring of employee activities. An algorithm may spot emerging sources of potential risk and alert managers so they can take preemptive action.[103] This is useful for enforcing workplace policies and identifying theft, fraud, and misuse of organizational information.[104] In industries with high rates of turnover, real-time monitoring also can reduce attrition by analyzing factors indicative of an impending resignation and predicting when an employee is considering leaving the company. Relevant factors identified by People Analytics include language patterns in emails and "suspicious" web traffic, such as increased visits to LinkedIn or Facebook, which, when tracked continuously, allow preemptive employer action.[105]

---

[101]   *See* Burdon & Harpur, *supra* note 66, at 690.

[102]   *See id.* at 688.

[103]   *See* Fineman, *supra* note 17. ("One of [Deloitte's] clients built a 'talent management dashboard' that analyzes 10 different measures of team engagement and performance, and delivers this information to all team leaders and senior managers throughout the company. . . . helping them understand hiring, management, and performance issues around the company in real time.").

[104]   *See* Tursunbayeva et al., *supra* note 11, at 224.

[105]   *See* Burdon & Harpur, *supra* note 66, at 689.

B. Market Forces Fail to Incentivize Improvements to Biased, Arbitrary, and Ineffective Algorithms

Predictive algorithms revolutionized baseball largely due to the quality and amount of publicly available baseball data, as well as the the ability to collect "objective measures of individual performance under well-specified conditions."[106] When applied to the ordinary workplace, however, algorithmic methodologies are more likely to exhibit bias that market competition cannot effectively or "reliably eliminate."[107] The laissez-faire argument that market forces will drive improvement or abandonment of biased and ineffective algorithms fundamentally misunderstands the mechanics of prediction and underestimates the disparity in bargaining power between employees and employers.

Employers rely on the developers of People Analytics software to program algorithms that will not discriminate against protected groups; however, this requires more than data cleansing and error correction. Even if programmers have no discriminatory intent, U.S. employment data nonetheless reflect the country's long history of structural discrimination, and predictions relying on complex statistical biases in the data may reproduce similar forms of systemic disadvantage to protected classes.[108] Eliminating such biases requires that the developer weigh sensitive ethical and policy tradeoffs and that the programmer have a deep understanding of the sources of structural racism and ways in which they manifest in the collected data.[109] It is unlikely that many private developers of algorithms will spend the necessary time and money on such an endeavor when they often do not even spend the resources necessary to ensure the accuracy of data.[110]

---

[106] *See* Kim, *supra* note 23, at 893.

[107] *See id.* at 894.

[108] *See id.* at 887.

[109] *See* Valentine, *supra* note 68, at 382–83 (discussing the political choices involved in tuning the rate of false positives generated by an algorithm).

[110] *See id.* at 388.

Moreover, discriminatory algorithms that reduce employers' costs are likely to persist in a competitive market because the employer and vendor will lack sufficient incentives to identify and eliminate bias.[111] One could imagine a predictive algorithm that effectively identifies some strong job candidates—and thus enhances organizational efficiency—even though the algorithm simultaneously excludes members of certain disadvantaged groups. If the algorithm's predictions align with the decision maker's "implicit assumptions or expectations," then "the same cognitive biases that data purportedly help to avoid may cause the human decision makers not to notice when the model is biased."[112] Additionally, for some professions and positions, comparing performance between workers is difficult due to a dearth of objective measures of performance.[113]

Even where objective measures are available, verification of the algorithm's accuracy through direct comparisons is often difficult, if not impossible. For example, in the selection context, employers rarely observe the "performance of [both] the accepted and [the] rejected candidates under identical circumstances," making it difficult to assess the benefit or veracity of the algorithm's guidance.[114] An alternative applicant, eschewed by the algorithm because of some deviation from the "ideal" candidate profile, may well have been more successful in the job than the chosen applicant, but the employer's People Analytics system never incorporates this counterfactual data. Employers have little incentive to question the algorithm's accuracy, particularly because market forces will "tend to affirm rather than disconfirm" the algorithm's usefulness.[115] The positive feedback effect produced by the apparent success of potentially biased or arbitrary predictions will contribute to the perceived accuracy

---

[111] *See* Kim, *supra* note 23, at 894.

[112] *See id.* at 895.

[113] *See id.* at 894.

[114] *See id.*

[115] *See* Katyal, *supra* note 9, at 90–91.

of the algorithm, and even a biased or arbitrary model may thereby become a self-fulfilling prophecy.[116]

Because objective academic research of People Analytics algorithms' causal inferences is incomplete, verification issues are more important.[117] It is possible that these models may base their predictions on factors misidentified as being causally connected to the organization's productivity target.[118] Indeed, some outside factor invisible to the algorithm may be the driving force behind the outcomes, which the algorithm interprets as confirmation of its accuracy.[119] Any unobservable or uncollected details about a worker's decisions, movements, or habits are invisible to the algorithm and thus eliminated from its calculus. For instance, algorithms designed to reduce attrition may ignore certain structural factors, like a decrease in alternative employment options, which could be influential in employees' decisions to stay on the job.[120]

C. Predictive Analytics' Focus on Algorithmic Profiling and Preemption

People Analytics make predictive inferences aimed at guiding employers' decisions to ostensibly maximize future organizational efficiency and profit. As employers take preemptive action against employees algorithmically determined to be threats to future profit, the profile characteristics from which those warnings were based will be increasingly stigmatized. The widespread adoption of these tools will accelerate intrusions into employee privacy and place significant powers of social control in the hands of large businesses.

Employers increasingly use People Analytics to profile individuals' future behavior, work performance, and

---

[116] *See* Kim, *supra* note 23, at 895–96.

[117] *See* Tursunbayeva et al., *supra* note 11, at 230.

[118] *See* Kim, *supra* note 23, at 895 (giving an example of the errors that can result from treating correlational algorithmic analysis as causal).

[119] *See id.*

[120] *See id.*

health.[121] The European Union's General Data Protection Regulation defines profiling as "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements."[122]

People Analytics algorithms group individuals together based on their qualitative attributes and habits, predict the future collective behavior of that group, and draw inferences on the basis of such predictions.[123] This creates a risk of statistical discrimination, or "discrimination by irrational correlation of information in which the discriminator bases a decision on a certain informational quality linked to the social or physical attribute of a given group."[124] In essence, an algorithm reduces individuals to assigned identities, group memberships, and statistical assumptions. Predictions from these elements increasingly govern the individual's opportunities, regardless of whether these group-based predictions are relevant to that individual.[125] Affected workers typically have no notice or opportunity to participate in the prediction process, which relies "primarily . . . on obscure data management and frequently takes place in situations of imbalance between data gatherers and data subjects."[126] Because "[e]mployers are under no duty to disclose the metrics used," workers are often unaware of what data others collect from them and how their employers measure performance.[127]

---

[121] *See* Wilson et al., *supra* note 12, at 3.

[122] Council Regulation 2016/679, art. 71, 2016 O.J. (L119) 1, 14.

[123] *See* Alessandro Mantelero, *Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection*, 32 COMPUT. L. & SEC. REV. 238, 239 (2016).

[124] *Cf.* Burdon & Harpur, *supra* note 66, at 694 (discussing statistical discrimination in a narrower context).

[125] *See* Balkin, *supra* note 65, at 1236–37.

[126] Mantelero, *supra* note 116, at 239.

[127] *See* Alexander & Tippett, *supra* note 79, at 995.

To be competitive, "compan[ies] ha[ve] to always collect new streams of data to produce new correlated patterns that provide new insights."[128] The relentless search for new sources of potentially business-relevant data has engendered attempts to quantify and analyze even unconscious human behaviors to provide additional insights into productivity maximization.[129] AI can conduct video interviews and "assess candidate honesty and personality" prior to any human interaction with a job applicant.[130] Vendors sell algorithms that "can pinpoint areas of potential fraud or client projects that are going poorly" by analyzing emails to identify an employee's mood and stress.[131] Some employers monitor workers' speech and movement.[132] "Sociometric badges" allow employers to "collect data on an employee's movements, [to] determine when employees are interacting, [to] analyze the tones of employees' voices, and then . . . break down quantitative data to determine which employees are interacting, where, for how long, and with what general type of emotional valence."[133]

As companies become more dependent on the complex analytical outcomes of predictive algorithms, "the prescriptive

128 Burdon & Harpur, *supra* note 66, at 686 (emphasis deleted).

129 *See* Josh Bersin, *People Analytics: Here with a Vengeance*, FORBES (Dec. 16, 2017, 11:39 AM), https://www.forbes.com/sites/joshbersin/2017/12/16/people-analytics-here-with-a-vengeance/#3ac746832a14 [https://perma.cc/5X6D-WJ4C].

130 *See* Fineman, *supra* note 17.

131 *See* Bersin, *supra* note 129.

132 Sprague, *supra* note 14, at 34 & n.129. Amazon promises employers that its Alexa for Business service will "let[] [their] employees be more productive throughout their day" by helping them "stay focused on important tasks whether at home, at work, or on the go." *Alexa for Business*, AMAZON WEB SERVS. (last visited Nov. 15, 2020), https://aws.amazon.com/alexaforbusiness/ [https://perma.cc/CV2E-XEY6].

133 Bodie et al., *supra* note 37, at 971. One researcher used data collected by sociometric badges equipped with microphones and motion detectors to conclude that certain types of employee interactions and interpersonal networks are key to enhancing "workplace loyalty and efficiency." *See id.* (citing BEN WABER, PEOPLE ANALYTICS: HOW SOCIAL SENSING TECHNOLOGY WILL TRANSFORM BUSINESS AND WHAT IT TELLS US ABOUT THE FUTURE OF WORK 109–21 (2013)).

focus of talent analytics could be central to future workplace recruitment and retention developments."[134] This focus could result in the "operationalisation, and potentially the automation, of decision-making predicated on predictive outcomes and probablised responses."[135] Algorithmic profiling thus tends toward "'a new truth regime', in which general strategies are adopted on a large scale on the basis of representations of society generated by algorithms, which predict future collective behaviour."[136] Reliance on algorithmic predictions gradually replaces the need for proof, and transparency and accountability in the decision-making process fall to the wayside.[137] As employers increasingly act based on algorithmically generated representations of society, a positive feedback loop emerges because the underlying database receives more and more data reinforcing the system's initial predictions.[138] Not only does this make it more difficult to question the validity of the algorithm's logic, but also it cedes increasing social and organizational control to the algorithm.[139]

Ian Kerr and Jessica Earle warn that, in the field of big data analytics, preemptive predictions "are intentionally used to diminish a person's range of future options" such that their use "as a means of avoiding risk becomes a catalyst for various

---

[134]   *See* Burdon & Harpur, *supra* note 66, at 692.

[135]   *See id.* at 687. The authors elaborate further:

> The prescripted employee therefore is an employee whose workplace behavioural patterns are increasingly being predicted. Future behaviour is predicted on an employee's own past actions and correlated against ranges of diverse data derived from unidentifiable populations of comparable employees. These predictions are thus founded on informational attributes that are increasingly random and unintuitive to both the employee and the employer.

Id. at 692.

[136]   *See* Mantelero, *supra* note 116, at 239–40 (footnote omitted).

[137]   *See id.* at 239–41 (discussing the issue in the general setting rather than the employment setting).

[138]   *See* Valentine, *supra* note 68, at 385–86 (giving examples).

[139]   *Cf. id.* at 368 (discussing government use of big data algorithms).

new forms of social preemption."[140] Vendors market People Analytics algorithms as productivity and strategy tools developed from the standpoint of the corporation to achieve organizational goals.[141] Even algorithms designed to impact employee morale aim at reducing the impact that low morale has on organizational productivity.[142] Thus, preemptive People Analytics algorithms are unlikely to adopt the perspective of the analyzed actor: the worker. [143] As the technology shifts towards more prescriptive uses, employers likely will consult algorithms for advice on "prescriptive outcomes that seek to modify human behavior to maximize operational benefits."[144] These algorithms will go beyond suggesting managerial actions to showing employers the future implications of each decision path.[145] Hence, the focus of these algorithms shifts from modeling probabilities to "facilitat[ing] the results of predicted outcomes."[146]

Employers' adoptions of predictive algorithms present a clear threat to individual autonomy, as well as norms of privacy and due process in the workplace, because

> [b]ig data enables a universalizable strategy of preemptive social decision-making. Such a strategy renders individuals unable to observe, understand, participate in, or respond to information gathered or assumptions made about them. When one considers that big data can be used to make important decisions that implicate us without our even knowing it, preemptive social decision making is antithetical to privacy and due process values.[147]

---

[140] Kerr & Earle, *supra* note 95, at 67, 69.

[141] *See* Tursunbayeva et al., *supra* note 11, at 229.

[142] *See* Eisenstadt, *supra* note 39, at 481–82 (giving an example of such an algorithm).

[143] *See* Kerr & Earle, *supra* note 95, at 67 ("Preemptive predictions are mostly made from the standpoint of the state, a corporation, or anyone who wishes to prevent or forestall certain types of action.").

[144] *See* Burdon & Harpur, *supra* note 66, at 686.

[145] *See id.*

[146] *See id.*

[147] *See* Kerr & Earle, *supra* note 95, at 71.

Despite this, predictive algorithms, including People Analytics systems, exist "in a regulatory vacuum."[148] Moreover, scholars warn that the normalization of preemptive prediction could result in the emergence of a new "duty to prevent," or "to mitigate future risk" using such predictions.[149] Using People Analytics, employers have substantial power to reshape the nature of work and the futures of individual workers through opaque and unaccountable means. Part IV will examine the dangers that algorithmic determinism poses to normative rights in the workplace.

IV. ALGORITHMIC PROFILING AND PREEMPTION IN THE WORKPLACE WILL ACCELERATE THE EROSION OF WORKERS' RIGHTS AND AUTONOMY

In the United States, the employment-at-will doctrine is the "unquestioned default rule in forty-nine" states.[150] In its current formulation, the employment-at-will doctrine allows businesses nearly "complete and unreviewable discretion to fire."[151] An employer has significant leeway to assess "whether [an] employee fits within the internal organization of the firm," and to base termination decisions on that judgment.[152] Moreover, scholars argue that today's workplaces effectively operate as "'private governments' with employers exercising near dictatorial power over what privacy rights may be granted to workers."[153] The applicability of federal surveillance statutes—like those prohibiting unlawful discrimination—to the employment context is "extremely

---

[148] Wilson, *supra* note 12, at 9.

[149] *See* Kerr & Earle, *supra* note 95, at 69–70.

[150] *See* Matthew T. Bodie, *The Best Way out Is Always Through: Changing the Employment At-Will Rule to Protect Personal Autonomy*, 2017. U. ILL. L. REV. 223, 227 (citing RESTATEMENT OF EMP. L. § 2.01 cmt. B (AM. L. INST. 2015))

[151] *See id.*

[152] *See id.* at 225–26.

[153] Ajunwa, *supra* note 60, at 49 (citing ELIZABETH ANDERSON, PRIVATE GOVERNMENT: HOW EMPLOYERS RULE OUR LIVES (AND WHY WE DON'T TALK ABOUT IT) 38–39, 41 (2017)).

narrow," and employers have "broad license to monitor employees."[154] Meanwhile, employees remain unaware of what data employers have and how they use it.[155]

Nonetheless, the rights to autonomy, due process, and the presumption of innocence extend normatively to the workplace. Scholars have argued that employers owe "the right to full information, the right to be heard, the right to ask questions and receive answers, and the right of redress."[156] State laws giving employees access to their own personnel files reflect these norms.[157] Other autonomy protections exist, but they "remain relegated to the public sector (through the First Amendment) or to state statutory schemes (such as off-duty laws)."[158] Thus, employees' enforceable rights vis-à-vis employers are highly dependent their employers and on state law and so vary widely.

Given the limited protections for normative employee rights, the novel harms presented by algorithmic technologies and the surveillance methods on which they rely may be unreachable by employment law. There are significant opportunities to use technology to enable "noncompliance [with employee protections], lawful avoidance strategies, and conduct that falls somewhere in between."[159] Workers already grappling with "tenuous ties to the labor force" will be

---

[154] *See* Ajunwa, *supra* note 60, at 50. As an example, Ajunwa notes, "[e]mployers could use data obtained from wellness programs to run predictive analytics of employee risk of injury. Thus, data from wearable[] [technology] will determine not only workers' compensation, but could influence which workers will remain employed." *Id.* at 51. No federal law would prevent this form of discrimination. *Id.*

[155] *See* Sprague, *supra* note 14, at 34.

[156] *See* Kerr & Earle, *supra* note 95, at 70.

[157] *See* JEROME G. SNIDER, HOWARD A. ELLINS & MICHAEL S. FLYNN, CORPORATE PRIVILEGES & CONFIDENTIAL INFORMATION § 11.03(2) & n.14, LexisNexis (database updated 2020) (discussing and listing these laws).

[158] *See* Bodie, *supra* note 150, at 226 (footnote omitted).

[159] *See* Alexander & Tippett, *supra* note 79, at 976.

particularly vulnerable to this trend, because labor laws will protect least these workers most in need of protection.[160]

A. The Dissolution of the Employee's Right to Privacy and Autonomy

Algorithmic profiling implicates substantial privacy and autonomy concerns, and the current regulatory landscape exacerbates them. Although there is no consensus, many scholars draw a connection between the right to privacy and the rights to personal autonomy and dignity.[161] Privacy, then, may be defined as control over the details of one's personal identity.[162] From a collective standpoint, privacy is necessary to "enable[] individuals both to maintain relational ties and to develop critical perspectives on the world around them."[163] Predictive analytics thus implicate workers' "privacy as control" because individuals cannot know how the data trails they leave will be used and what that data will predict.[164]

People Analytics imbues data collected outside the workplace with new meaning by identifying novel correlations between business outcomes and previously unquantifiable or seemingly irrelevant factors.[165] At the same time, digital technologies have rapidly revolutionized surveillance and data collection.[166] Companies now easily purchase and aggregate data from a broad array of sources, both in the workplace and far beyond it.[167] Consequently, U.S. employers today have access to substantial pools of data about workers

---

[160] *Cf. id.* at 1012 (observing that "marginal workers" are likely to perceive "no protection at all" when businesses use technology to avoid employer-employee relationships).

[161] *See, e.g.*, Katsabian, *supra* note 79, at 233–34 (discussing Daniel Solove's approach).

[162] *See* Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977).

[163] *See* Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1906 (2013).

[164] *See* Spencer, *supra* note 1, at 629.

[165] *See supra* notes 90–94 and accompanying text.

[166] *See* Bersin, *supra* note 129 (giving examples).

[167] *See* Kim, *supra* note 58, at 406.

that historically would have been considered too personal, private, or irrelevant to be used for business purposes.[168]

Employers now see substantial value in developing new techniques to collect, analyze, and exploit a broader array of employee data, often without notice to the employee.[169] Deloitte reports that "[t]he use of external data for [P]eople [A]nalytics has grown significantly, as more than 50 percent of companies now actively use social network and external data to understand attrition, retention, and other performance metrics."[170] Additionally, a growing number of companies have introduced wearable technologies, like Fitbits or microchip implants, which monitor employees and amass detailed behavioral and health data.[171] Employers—sometimes through "wellness programs"—encourage employees to wear these devices and make their data available to the employer.[172] This creates opportunities for both employers and private wearable technology companies to aggregate and repurpose the data they collect from participating employees.

The Fourth Amendment protects an individual's "reasonable expectation of privacy" as measured against "broadly based and widely accepted community norms."[173] The application of this standard to employers' new data collection methods remains uncertain.[174] However, there is some authority rejecting an expectation of privacy in the use

---

[168] *See* Matthew T. Bodie, *Workplace Freakonomics*, 14 I/S 37, 43–44 (2017).

[169] *Cf. id.* at 38–39 (discussing potential advantages of wider-ranging use of data).

[170] Fineman, *supra* note 17.

[171] *See* Ajunwa, *supra* note 60, at 36–42.

[172] *See id.* Professor Ajunwa cautions that wearable devices pose a particularly "high risk of challenging basic privacy principles," including "collection limitation, purpose specification, use limitation, accountability, security, notice, choice, and data minimization," because many of these devices "lack input mechanisms and extensively collect, store, and transmit personal data on a cloud." *Id.* at 42–43.

[173] *See id.* at 49 (internal quotation marks omitted) (quoting Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078, 1091 (N.D. Cal. 2018)).

[174] *See id.* at 49–50.

of employer-owned property during business hours.[175] Moreover, "employees routinely sacrifice personal privacy for the sake of convenience,"[176] contributing to the erosion of the privacy norm and thereby narrowing the "reasonable" sphere of privacy.

For instance, employers may use data obtained from workplace wellness programs and wearable technologies to run predictive analytics assessing employees' risk of future injury.[177] Without the worker's knowledge or consent, employers could use these data not only to determine the worker's compensation but also to influence the employers' promotion, training, and termination decisions.[178]An algorithm might flag an employee due to her weight or her addiction to cigarettes, without hindrance from federal law.[179] Moreover, employers "frequently [sell wearable data] to third parties without the employee's knowledge or consent."[180]

Traditional forms of privacy protection are unlikely to protect workers from biased or arbitrary predictions of People Analytics algorithms.[181] Long-term data tracking and analysis by private parties "is now ubiquitous and fundamentally unavoidable."[182] The privacy challenges from data aggregation presented by diverse sources extend beyond the information gleaned from by individual data streams. By combining substantial quantities of data from a wide variety of sources and mining the data through analytics processes that identify implicit patterns, employers can uncover "'new facts,' relationships, or associations about a person, placing that person in a 'newly discovered' category or group."[183]

---

[175] *See id.* at 50 & n.248.

[176] Eisenstadt, *supra* note 39, at 470.

[177] Ajunwa, *supra* note 60, at 51.

[178] *See id.*

[179] *Id.*

[180] *See id.*

[181] *See* Kim, *supra* note 23, at 897–98.

[182] *See* Sprague, *supra* note 14, at 25.

[183] *Id.* at 20 (quoting HERMAN T. TAVANI, ETHICS AND TECHNOLOGY: CONTROVERSIES, QUESTIONS, AND STRATEGIES FOR ETHICAL COMPUTING 151 (4th ed. 2013)).

Thus, "the disclosure of relatively trivial bits of information may reveal far more sensitive information when data is aggregated and analyzed."[184]

Some have suggested that the Fair Credit Reporting Act (FCRA) may provide a helpful model for regulating predictive analytics in the workplace.[185] "The FCRA requires an employer to obtain an applicant's consent before it accesses a consumer report, to provide notice of an adverse action based on a consumer report along with a copy of the report, and to provide information about the individual's rights to dispute the report's accuracy."[186] Currently, the FCRA "put[s] few obstacles in the path" of employers using "consumer data to make personnel decisions."[187]

Moreover, critics have flagged several flaws in the FCRA system that are likely to affect FCRA-style regulation of People Analytics. For instance, notice and consent provide doubtful protection for privacy interests. "[A]pplicants have little choice but to consent to the use of credit reports if they wish to be considered for a job,"[188] and the same may be true of consent to People Analytics. Further, because of the scope of big data analytics today, the "consent obtained at the moment data is collected is not meaningful, given that it is

---

[184] Kim, *supra* note 23, at 900. The judiciary has begun to recognize the intrusive potential of stored data and inferences derived from analysis of that data. In one Fourth Amendment case, Chief Justice Roberts noted that

> [a]n Internet search and browsing history . . . could reveal an individual's private interests or concerns . . . . Data on a cell phone can also reveal where a person has been. Historic location information . . . can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Riley v. California, 573 U.S. 373, 395–96 (2014).

[185] *See* Sprague, *supra* note 14, at 42–43 (suggesting the model and possible extensions).

[186] Kim, *supra* note 23, at 899 (footnote omitted).

[187] *Id.*

[188] *Id.*

impossible to know all subsequent uses of that information and its impact in advance."[189]

FCRA-style legislation also will fail to address other impacts on worker autonomy. Because weak consent is easy to obtain, programmers and employers may deploy People Analytics in socially manipulative ways. In fact, armed with additional knowledge about the People Analytics system, workers may internalize the algorithm's classifications and risk assessments, leading them to alter their identities or behavior in an attempt to reclassify themselves in a more desirable category, appear less risky to the company, or refrain from certain activities to escape algorithmic oversight.[190] Employers will also retain the ability to use the algorithms to incentivize workers to make predictable choices and, over time, better understand "which people are most susceptible to manipulation, and how they can most easily and effectively be manipulated."[191] If an algorithm determines that high predictability and manipulability are key to profit maximization, no law would prevent employers from using such metrics to determine which candidates and employees are a good fit for the company.[192] Such systemic threats to workers' autonomy and dignity are difficult, if not impossible, to address through data privacy legislation (whether modeled on the FCRA or otherwise) alone.

B. The Inadequacy of Anti-Discrimination Regulations to Combat Algorithmic Bias

As discussed in Part III, algorithms are vulnerable to statistical bias, particularly because they may rely on "biased, error-ridden, or unrepresentative data."[193] However, traditional tools for responding to discrimination are less effective against structural biases perpetuated by predictive

---

189   *See id.* at 900.

190   *See* Balkin, *supra* note 65, at 1238–39.

191   *See id.* at 1239.

192   *Cf. supra* notes 145–49 (discussing at-will employment).

193   *See* Kim, *supra* note 23, at 887; *see also supra* text accompanying notes 107–109.

algorithms.[194] This is, in part, because bias "created by algorithmic decision-making, even if it tracks constitutionally prohibited prejudice, is masked by outwardly neutral proxy variables coded into the systems."[195] People Analytics reproduces systemic disadvantages through opaque conclusions often driven by unknown or unexplained correlations among data,[196] making it difficult to spot and challenge "this sort of algorithmic 'rational' racism" even though its discriminatory effects "can be as destructive as overt prejudice."[197] Shielding details about an individual's genetic condition or disability status from analysis does not prevent an algorithm with access to large amounts of behavioral data from inferring protected information or giving substantial weight to a proxy for a protected characteristic.[198] Predictions based on such inferences may guide the employer's personnel decisions.[199]

1. The Uniform Guidelines on Employee Selection Procedures

Federal regulations of potentially discriminatory employment practices fail to reach predictive People Analytics algorithms. For instance, since 1978, the Equal Employment Opportunity Commission (EEOC) and other federal agencies have relied upon the Uniform Guidelines on Employee Selection Procedures (UGESP) to assess the legality of applicant screening and selection tests.[200] Employers may consider a "credential or test that disparately affects a protected group if the credential or test predicts success in the

---

[194] *See* Kim, *supra* note 23, at 890–91.

[195] Valentine, *supra* note 68, at 383.

[196] *See* Kim, *supra* note 23, at 889.

[197] *See* Valentine, *supra* note 68, at 383.

[198] *See* Kim, *supra* note 23, at 898. Kim notes further that prohibitions on access to sensitive information could actually exacerbate an algorithm's propensity towards classification bias due to the problem of omitted variable bias. *See id.* at 898–99.

[199] *See id.* at 885 (discussing cost-based decisions founded on inferences about medical risks).

[200] *See* 29 C.F.R. §§ 1607.1–1607.18 (2020).

position for which it is used."[201] The UGESP "offer employers various means of validating tests," and the applicable means depend "on what the test seeks to measure (e.g., personality traits, job tasks, or skills associated with job success)."[202]

People Analytics algorithms designed to assess job candidates use "reams of data to 'predict' who is a good hire," a process which "is conceptually indistinguishable from using a written test to identify aptitude for a job."[203] However, the EEOC designed the UGESP to regulate pre-digital testing models, which were "heavy on theory but short on evidentiary support," so the guidelines are "intended to demand a baseline quantum of evidence to support the application of theoretical models."[204] Since People Analytics relies on analysis of correlations among data, this underlying data likely will be viewed as sufficient evidentiary support to justify an algorithm's use under the UGESP.[205] For this reason, scholars predict that the UGESP will be "ineffective" in monitoring selection algorithms.[206]

---

201   Bodie et al., *supra* note 37, at 1023.

202   Alexander & Tippett, *supra* note 79, at 996. The UGESP divides screening and selection tests into three categories, each with their own validation procedures: (1) tests gauging employee traits, such as personality or IQ, are measured for "construct validity"; (2) tests involving tasks required by the job itself (measured for "content validity"), and (3) tests gauging "knowledge of skills predictive of success on the job," such as production rate, are (measured for "criterion validity"). *See* 29 C.F.R. § 1607.14. The latter two validation procedures typically require "testing the measure on a sample of workers representative of the 'relevant labor market' to verify whether the measure is in fact predictive of success on the job." *Id.* at n.118. *See also id.* 29 C.F.R. § 1607.16(D), (F).

203   Alexander & Tippett, *supra* note 79, at 995–96.

204   *See id.* at 997.

205   *See id.*.

206   *See id.* (citing Kim, *supra* note 23, at 879–80 (explaining that data mining is atheoretical insofar as "[d]ata miners have no particular theory they are trying to test, nor are they necessarily interested in explaining observed relationships between different variables")).

2. Title VII

Some scholars opine that current Title VII doctrine "appear[s] to bless" the use of algorithms that work to disadvantage protected groups in many cases.[207] However, Professor Pauline Kim has proposed interpreting Title VII to better protect employees from algorithmic bias, adapting traditional disparate impact so that "an employer [who] relies on a data-driven classification scheme to sort applicants or employees . . . should be responsible for the impact that selection device has on the opportunities of workers in protected classes."[208] This would require the judiciary to extend Title VII's prohibitions on discrimination to what Kim describes as "classification bias."[209] Kim also urges changes in the law to provide workers with meaningful opportunities for relief, including making "an employer's defense of an algorithm with biased effects . . . depend, not on a claim of job-relatedness, but on the employer proving that the underlying model is statistically valid and substantially meaningful."[210]

V. TOWARDS TRANSPARENT AND ACCOUNTABLE PEOPLE ANALYTICS

Although European privacy regulations attempt to restrict automated decisionmaking and decisionmaking based on algorithmic profiling,[211] the United States has been much slower to respond to the autonomy-compromising applications of algorithms: current data privacy legislation also contains broad exemptions for employer use of employee data.[212]

Even if these data privacy laws expand to cover employers, merely preventing an employee's data from entering a

---

[207] *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 672 (2016).

[208] *See* Kim, *supra* note 23, at 917.

[209] *See id.* at 917–18.

[210] *See id.* at 917, 920–922.

[211] *See* Council Regulation 2016/679, art. 71, 2016 O.J. (L119) 1, 14.

[212] *See e.g.*, California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.120, .140 (2020) (allowing certain business transactions in data with "service providers" even when an individual opts out of data sales).

particular data pool will not protect that employee from the privacy intrusions of algorithmic profiling or from the resulting discriminatory and arbitrary limitations on freedom of choice and opportunity. Even an employee who has exercised her newly-granted right to opt out of the resale of her data may, depending on workplace policy, still feel the influence of her employer's People Analytics algorithm. The algorithm will identify a profile that the employee is likely to fit and use that profile to guide or control decisions which may affect her employment status, opportunities, or her cost of employer-provided healthcare.[213] The only difference is that the algorithm no longer uses the employee's own data, increasing the likelihood that the algorithmically-developed profile will provide less accurate predictions regarding that employee. Laws which so narrowly frame the harms of data privacy exploitation risk undermining our ability to conceptualize and address the significant threats that data mining poses to individual and collective autonomy in the workplace and beyond.[214]

A. Regulatory Priorities

Algorithmic transparency is a necessary step towards understanding how to regulate and monitor effectively the abuse of predictive analytics in the workplace without unnecessarily sacrificing technological development or the benefits that could be derived from algorithmic insights.[215] People Analytics processes are largely invisible to those whose freedoms they restrict.[216] Applicants and employees typically have no right to notice or explanation, no opportunity to consent, and no practical ability to dispute the applicability,

---

[213] *Supra* Section V.B.

[214] *See* Kerr & Earle, *supra* note 95, at 71.

[215] *See* Balkin, *supra* note 65, at 1239.

[216] *See* Bloch-Wehba, *supra* note 75, at 1272.

efficacy, or disparate impact of the methodology underlying their employers' algorithms.[217]

Predictive analytics systems—including the underlying database and the algorithmic source code—are highly opaque.[218] "Businesses routinely guard both the database (as well as the predictive system itself) as trade secrets, and even when the database is available, you typically do not know what data was discarded or altered in the processes of collection, selection, cleaning, and structuring."[219] Even if a plaintiff obtains access to the algorithm, it is often so complex that expert testimony is required to understand how the system operates.[220]

Ideally, regulations should ensure that People Analytics algorithms are both explainable and transparent. Some algorithms are "explainable" in the sense that it is possible to "provide an adequate, human-understandable characterization and explanation of [their] classifications and predictions," but some algorithms are not.[221] Algorithmic "transparency" requires that details about the construction of the algorithm be available.[222] These details include information about the training data, the methodology, the source code, and the data set being used to inform the application of the algorithm to the workplace.[223] Transparency requires limiting the scope of trade secrets protections.[224]

A worker's autonomy might be preserved to some extent by improving her access to information so that she can make

---

[217] *See* Crawford & Schultz, *supra* note 21, at 98 (illustrating the notice and consent issues with an example); *supra* text accompanying notes 188–97.

[218] Robert H. Sloan & Richard Warner, *Algorithms and Human Freedom*, SANTA CLARA HIGH TECH. L.J., Apr. 2019, at 19.

[219] *Id.*

[220] *See id.*

[221] *Id.* at 20. For instance, deep neural nets and support vector machines tend to be so complex that their outputs are not explainable. *Id.*

[222] *Id.* at 20–21.

[223] *See id.* at 19–22.

[224] *See id.* at 22.

informed decisions and dispute inaccurate results. As Professor Kerr points out, "if one essential element of any just decision-making process is its predictability, then it must be possible for the subjects of those predictions—whose life chances and opportunities are in the balance—to scrutinize and contest the projections and other categorial assumptions at play within the decision-making processes themselves."[225] Thus, regulations should attempt to reduce the extreme informational asymmetries which now exist between the employee and the employer. Employees should receive notice when an algorithm may alter the choices and opportunities available to them. Further, workers and unions should have a right to an explanation of how a relevant algorithm functions, including a description of its training data, its target variables, and its inferences from correlations.

B. The Importance of Employee Voice and Collective Action

The threats posed by faulty and discriminatory predictive algorithms are too urgent for workers to rely on future protections from federal and state legislation, particularly in the current political climate of partisan gridlock[226] and substantial donations from technology companies.[227] Even where existing legal partiregimes may provide some opportunity for challenging these algorithms, the liability model is not well suited to address the structural harms of algorithmic bias.[228] Individuals are often unaware of the ways in which a predictive algorithm controls their employment opportunities and, even if they become aware, the arbitrary nature or discriminatory impact of the algorithm may be

---

[225] Kerr, *supra* note 98, at 111.

[226] Derek Willis et al., *How Congress Stopped Working*, PROPUBLICA (Nov. 5, 2018), https://www.propublica.org/article/how-congress-stopped-working [https://perma.cc/T5TS-2JAG].

[227] *See* Sissi Cao & Jordan Zakarin, *Big Tech and CEOs Poured Millions Into The Election. Here's Who They Supported*, OBSERVER (Nov. 2, 2020), https://observer.com/2020/11/big-tech-2020-presidential-election-donation-breakdown-ranking/ [https://perma.cc/MW4Q-6LKH].

[228] *See* Kim, *supra* note 23, at 933–34.

hidden.[229] To detect and pursue a claim of bias is "highly resource- and time-intensive," and most plaintiffs will be unable to afford such costs.[230]

Scholars have recognized immediate value in reinforcing even non-legal norms of transparency, disclosure, and autonomy to encourage the ethical development and use of People Analytics.[231] Historically, employee voice has been critically important in guiding "workplace law, norms, and business policy."[232] Both the NLRA and some employee-centered management practices facilitate and reflect the importance of employees' normative rights "to exercise collective voice over their terms and conditions of employment."[233] Worker protests and strikes provided the impetus for regulatory restrictions curtailing older forms of workforce analytics, like Taylorism, which workers found unreasonably intrusive and inhumane.[234]

Transparency and employee voice also could enhance corporate accountability and fairness. Employees ought to be involved in the design and implementation of the People Analytics algorithms to which they will be subject.[235] Employer transparency would likely result in less worker alienation and thus contribute to the sustainability of these

---

[229] *See id.*

[230] *See id.* at 934.

[231] *See, e.g.*, Bodie et al., *supra* note 37, at 1032. Redefining and strengthening norms to protect individuals and society from novel risks presented by emerging technologies can be helpful, not least because it may provide a frame through which regulators may approach the problem. For instance, Sloan and Warner propose a norm-based strategy for FTC regulation of predictive analytics. *See* Sloan & Warner, *supra* note 218, at 32–34.

[232] *See* Bodie et al., *supra* note 37, at 1032.

[233] *See id.* at 1032–33.

[234] *See* Sprague, *supra* note 14, at 45 (describing the effects of a strike on Taylorism).

[235] *See* Bodie et al., *supra* note 37, at 1037 ("Workplaces that wish to experiment with [P]eople [A]nalytics would be wise to include employees in the process and design, providing opportunities for input.").

algorithms as useful tools for organizational strategy.[236] "[W]hen employees are concerned with how the [employer] handles their private information and consider the organizational information privacy practices to be less legitimate, such concerns also translate into lower commitment to the organization."[237]

VI. CONCLUSION

Algorithmic outputs based on statistical profiling now guide or supplant human decisionmaking in a wide variety of fora, often with determinative effects on individuals' freedom of choice and opportunity. Despite the significant impact that these algorithms will have on our lives, their likely discriminatory or arbitrary effects, and the potential for their proprietors to intentionally or accidentally manipulate human behavior en masse,[238] few have challenged the absence of accountability. Developers, empowered by trade secrets law, staunchly refuse to reveal the source code of these tools that are shaping our future.

Employee voice and algorithmic transparency would facilitate refinement of People Analytics to achieve more accurately and efficiently its intended goals, address biases overlooked by developers, and ensure that employees' rights to autonomy and privacy receive protection at every stage of the algorithmic process. Transparency would also provide a means by which employees could hold their employers accountable when algorithmic insights are wielded in an arbitrary or unfairly determinative manner. Individuals'

---

[236] *See id.* at 1036–37 ("When employees hold more positive attributions—that is, when they consider [P]eople [A]nalytics as a means to improve quality for customers or to enhance employee well-being—such attributions relate positively to their affective commitment [to their employer].").

[237] *Id.* at 1037 (footnote omitted).

[238] *See* Marcello Ienca & Effy Vayena, *Cambridge Analytica and Online Manipulation*, SCI. AM. (Mar. 30, 2018), https://blogs.scientificamerican.com/observations/cambridge-analytica-and-online-manipulation/ [https://perma.cc/G7J6-R479] (describing the use of algorithms to manipulate emotions and political results).

access to choices and opportunities should not be withheld simply because they fall on the wrong side of a questionable statistical inference. If enhanced productivity and labor market efficiency are truly the business goals of algorithmic decisionmaking, then the exacerbation of informational disparities is not a rational solution.