ARTICLES

The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance, Under the Labor Laws

Richard A. Bales† & Katherine V.W. Stone††

Employers and others who hire or engage workers to perform services use a dizzying array of electronic mechanisms to make personnel decisions about hiring, worker evaluation, compensation, discipline, and retention. These electronic mechanisms include electronic trackers, surveillance cameras, metabolism monitors, wearable biological measuring devices, and implantable technology. With these tools, employers can record their workers' every movement, listen in on their conversations, measure minute aspects of performance, and detect oppositional organizing activities. The data collected is transformed by means of artificial intelligence (AI) algorithms into a permanent electronic resume that can identify and predict an individual's performance as well as their work ethic, personality, union proclivity, employer loyalty, and future health care costs. The electronic resume produced by AI will accompany workers from job to job as they move around the boundaryless workplace. Thus AI and electronic monitoring produce an invisible electronic web that threatens to invade worker privacy, deter unionization, enable subtle forms of employer blackballing, exacerbate employment discrimination, render unions ineffective, and obliterate the protections of the labor laws.

This article describes the many ways AI is being used in the workplace and how its use is transforming the practices of hiring, evaluating, compensating, controlling, and dismissing workers. It then focuses on five

†. Richard A. Bales is a Professor of Law at Ohio Northern University and a Visiting Professor of Law (2018–20) at the University of Akron Law School. He would like to give special thanks to Susan Mary Altmeyer, University of Akron Law School, for her help on section II-C.

††. Katherine V.W. Stone is the Arjay and Frances Fearing Miller Distinguished Professor of Law at UCLA School of Law. She thanks Adrian Butler of UCLA School of Law for exceptional research assistance.

areas of law in which AI threatens to undermine worker protections: anti-discrimination law, privacy law, antitrust law, labor law, and employee representation. Finally, this article maps out an agenda for future law reform and research.

INTRODUCTION

Although the workplace has become boundaryless, it has not become random.[1] Today, workers have many different types of relationships with companies, from conventional long-term employment to the occasional project or "gig." They often have multiple interlocking and cascading tiers of employers all at once,[2] and employee leasing firms, payroll contractors, human resources (HR) service providers, and numerous types of ancillary enterprises also perform employer functions. Workers perform their services in many different locations, including their homes, coffee shops, private automobiles, or WeWork shared spaces. But while the location may be flexible, the job fluid, and the identity of the employer elusive, the worker operates within an invisible electronic web that measures, quantifies, analyzes, and ultimately shapes essential features of the work experience.

Employers and others who hire, retain, or engage workers to perform services utilize a dizzying array of electronic mechanisms—including trackers, listening devices, surveillance cameras, metabolism monitors, and wearable technology—to watch their workers, measure their performance, avoid disruption, and identify shirking, theft, or waste. These mechanisms can observe each worker's every movement, both inside and outside the workplace, and during and after working hours. The data collected are transformed by means of artificial intelligence (AI) algorithms into a permanent electronic resume that companies are using to track and assess current workers, and it could potentially be shared among companies as workers move around the boundaryless workplace from job to job. This

1. A "boundaryless workplace" is one in which the long-term bond between workers and employers has become attenuated and employees more readily from one to another. *See generally* KATHERINE V.W. STONE, FROM WIDGETS TO DIGITS: EMPLOYMENT REGULATION FOR THE CHANGING WORKPLACE 2004). *See also* Katherine V.W. Stone, *Legal Protections for Atypical Employees: Employment Law for Workers Without Workplaces and Employees without Employers*, 27 BERKELEY J. EMP. & LAB. L. 251 (2006); Katherine V.W. Stone, *A Fatal Mis-Match: Employer-Centric Benefits in a Boundaryless Workplace,* 11 LEWIS & CLARK L. REV. 451 (2007); Katherine V.W. Stone, *Employee Representation in the Boundaryless Workplace,* 77 CHI.-KENT L. REV. 773 (2002). The author selected the term "boundaryless workplace" to evoke and build upon the concepts of a "boundaryless career," as used in the organizational behavior field, and the notion of a "boundaryless company," as discussed in the field of management. *See* STONE, FROM WIDGETS TO DIGITS, *supra*, at 92–94 and references cited therein.

2. *See* DAVID WEIL, THE FISSURED WORKPLACE: WHY WORK BECAME SO BAD FOR SO MANY AND WHAT CAN BE DONE TO IMPROVE IT 223 (2014).

invisible electronic web threatens to invade worker privacy, deter unionization, enable subtle forms of employer blackballing, exacerbate employment discrimination, render unions ineffective, and obliterate the protections of the labor laws.

This article maps developments in AI as well as the dangers posed by the spread of AI and electronic data gathering in the workplace. In Part I, we discuss the growing use of AI and electronic data gathering in HR practices. After describing the enormous potential and many uses of AI, we describe how AI's use in the workplace has transformed the practices of hiring, evaluating, compensating, and dismissing workers. We also discuss the emerging types of electronic devices used to gather the data necessary to the operation of AI.

In Part II, we analyze the legal issues that arise from the invisible web of HR-oriented AI that increasingly permeates the boundaryless workplace. Specifically, we focus on four areas in which AI threatens to undermine worker protections: anti-discrimination law, privacy law, antitrust law, and labor law. We also consider the challenges AI poses for unions in their role of protecting workers and promoting workplace justice.

In Part III, we conclude with an agenda for future research and some proposals for legal reform. These include research on whether and how AI may have a discriminatory effect on minorities, women, or other disadvantaged groups when it is deployed for monitoring, career-tracking, disciplining, and firing workers; expanding worker privacy rights to give workers more protection in the collection and use of their personal and professional data; antitrust restrictions on the ability of companies to share workers' personal and professional data; and a clear duty on employers to disclose AI linked surveillance and to bargain with unions over workplace monitoring and data collection.

II. THE INVISIBLE WEB: AI IN THE WORKPLACE

A. Human Resources by Algorithm

Artificial intelligence (AI) is everywhere: Alexa is in our homes, autonomous vehicles are prevalent in mining and agriculture,[3] and AI is increasingly making personnel decisions in the workplace.[4] AI likely will disrupt every context it touches. In the workplace, for example, it will eliminate broad categories of jobs, create broad categories of new ones, and

3. Alex Davies & Aarian Marshall, *Are We There Yet? A Reality Check on Self-Driving Cars*, WIRED (Apr. 22, 2019, 6:00 AM), https://www.wired.com/story/future-of-transportation-self-driving-cars-reality-check/ [https://perma.cc/G47V-8P4J].

4. *See infra* Part I.B.

transform others.[5] Indeed, to say that AI will transform the workplace[6]—and the world—as we know it is a significant understatement. A report from the International Bar Association calls it the fourth industrial revolution.[7] An equally apt description might be a fourth era in production.[8]

Employers already are using AI to screen job applications, interview and assess applicants, track the physical movement of workers, assess performance and recommend promotions and pay rates, and monitor workers' emails and phone calls and non-worktime social media activity.[9] But the laws governing the workplace largely predate the digital age and are not adequate to address the challenges it poses.[10]

1. The Vast and Enlarging Scope of AI Capabilities in the Production Process

a. Data Mining and Deep Learning

AI has been defined as "a branch of computer science dealing with the simulation of intelligent behavior in computers."[11] AI gathers and analyzes huge troughs of data and uses it to sense, comprehend, act, and learn.[12] AI is a large category that includes machine learning, pattern recognition, problem solving, and adaption to changing circumstances.[13]

---

5. *See generally* AJAY AGRAWAL, JOSHUA GANS, & AVI GOLDFARB, PREDICTION MACHINES: THE SIMPLE ECONOMICS OF ARTIFICIAL INTELLIGENCE (2018); PAUL R. DAUGHERTY & H. JAMES WILSON, HUMAN + MACHINE: REIMAGINING WORK IN THE AGE OF AI (2018).

6. *See AI-spy: The Workplace of the Future*, THE ECONOMIST (Mar. 28, 2018), https://www.economist.com/leaders/2018/03/28/the-workplace-of-the-future [https://perma.cc/UU4K-JLSL]; *Hire Education: Managing Human Resources is About to Become Easier*, THE ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/managing-human-resources-is-about-to-become-easier [https://perma.cc/4A5R-DQ8J]; *see also* Jeffrey M. Hirsch, *Future Work*, U. ILL. L. REV. (forthcoming 2020) [introduction] (suggesting that technology's potential to disrupt the labor market may have reached a "tipping point" risking labor unrest and violence).

7. INT'L BAR ASS'N GLOB. EMP'T INST., ARTIFICIAL INTELLIGENCE AND ROBOTICS AND THEIR IMPACT ON THE WORKPLACE 11 (Apr. 2017) ("IBA"). The first was industrialization; the second was electrification; the third was digitalization. *Id.*

8. *See* Katherine V. W. Stone, *Rupture and Invention: The Changing Nature of Work and the Implications for Social Policy*, CAMBRIDGE HANDBOOK OF US LABOR LAW: REINVENTING LABOR LAW FOR THE 21ST CENTURY (Richard Bales et al., ed., forthcoming 2020). The first was artisanal production; the second was industrial production; the third was digital production; the fourth is a new era of workplace production.

9. *See infra* Part II.

10. *AI-spy*, *supra* note 6 ("Few laws govern how data are collected at work . . . .").

11. *Artificial Intelligence*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/artificial%20intelligence [https://perma.cc/NN3L-2F5L] (last visited Nov. 3, 2019).

12. DAUGHERTY & WILSON, *supra* note 5, at 3.

13. Bernard Marr, *The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance*, FORBES (Feb. 14, 2018, 1:27 AM), https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/#72f42e084f5d [https://perma.cc/9KVA-A6EC].

The volume of stored data is immense and growing exponentially.[14] Although data sets can have economic value in their own right[15] (consider Facebook's sale of data to makers of mobile phones and other devices[16]), the highest-level value is in analyzing that data to predict future behavior based on detectable patterns.[17] This is accomplished by using data to create a set of algorithms that attempt to model high-level abstractions.[18] For example, feed a computer a million images of cats with the label "cat," along with a similar number of images of other animals without the "cat" label, and the machine will "learn"[19] through trial and error to distinguish cats from other four-legged creatures.[20] Feed enough medical images to a computer and the job of radiologist may become obsolete.[21]

Key to the recent explosion of AI is rapidly increasing computer power and the decreasing cost of harnessing it.[22] As the cost of processing data decreases, the ability to use existing data to create new data—and to make predictions—increases. These predictions can be used to control autonomous cars,[23] manage supply chains,[24] and monitor peoples' abilities, actions, and

14. By one estimate, the worldwide volume of data is expected to be more than 100 zettabytes (100,000,000,000,000,000,000,000) in 2020, ten times the volume in 2006. IBA, *supra* note 7, at 99 (citing BITKOM, *Big Data im Praxiseinsatz — Szenarien, Beispiele, Effekte* 12 (2012), https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2012/Leitfaden/Leitfaden-Big-Data-iAIm-Praxiseinsatz-Szenarien-Beispiele-Effekte/BITKOM-LF-big-data-2012-online1.pdf [https://perma.cc/D3CR-FWYY]).

Consumers and workers often do not realize when and how their data are being collected and used. *See, e.g.*, Maria Armental, *Apple Tightens Privacy Rules on Siri Recordings After Backlash*, WALL ST. J. (Aug. 28, 2019, 4:00 PM), https://www.wsj.com/articles/apple-tightens-privacy-rules-on-listening-to-siri-recordings-11567013482 [https://perma.cc/54J4–2FWZ] (discussing Apple's use of Siri to surreptitiously record and retain audio conversations about sensitive subjects such as medical conditions). This, in turn, makes it possible to monitor workers in ways they may not immediately recognize. Just as a Roomba's memorizing the configuration of our house seems innocuous until we realize that data are being sent to Roomba Inc., wearing a "smart" nametag that gives you access to locked doors in the workplace seems innocuous until you realize it's also tracking every minute you spend in the bathroom and every person you talk to throughout the day. *See generally infra* Part 0.

15. IBA, *supra* note 7, at 107 (characterizing data as "the oil of the future") (internal quotation marks omitted).

16. Gabriel J.X. Dance, Nicholas Confessore & Michael LaForgia, *Facebook Gave Device Makers Deep Access to Data on Users and Friends*, N.Y. TIMES (Jun. 3 2018), https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html [https://perma.cc/62T2-ZSTM].

17. AGRAWAL ET AL., *supra* note 5, at 23–51.

18. IBA, *supra* note 7, at 10.

19. *See* DAUGHERTY & WILSON, *supra* note 5, at 60–63 (describing different types of machine learning).

20. AGRAWAL ET AL., *supra* note 5, at 38.

21. *Id*. at 145–48.

22. AGRAWAL ET AL., *supra* note 5, at 11–17.

23. *See, e.g.*, X. Du et al., *Bio-LSTM: A Biomechanically Inspired Recurrent Neural Network for 3-D Pedestrian Pose and Gait Prediction*, [4, No. 2] IEEE ROBOTICS AND AUTOMATION LETTERS 1501, 1501–1508 (2019), https://ieeexplore.ieee.org/document/8626436 [https://perma.cc/QU7E-NHDT].

24. *See, e.g.*, Steve Banker, *20 Things To Know About Artificial Intelligence For Supply Chain Management*, FORBES (Jan. 1, 2019, 4:54 AM),

proclivities.[25] From 2015 to 2017, the value of AI-related mergers and acquisitions increased about 26-fold, to $22 billion.[26] The corporate market for AI software, hardware, and services is forecast to grow from $12 billion in 2017 to $58 billion in 2021.[27] This investment money is being channeled into data mining and deep learning, robotics, computer vision, and speech recognition.

b. Robotics and AI

Robots are hardly new on the factory floor. From assembly-line conveyor belts to robotic arms, machines used to perform discrete tasks have been a staple of factories for more than a century.[28] In the 1940s and 1950s, numerically controlled machines that could perform multiple and reprogrammable tasks were introduced. In the mid-1970s, computerized numerically controlled (CNC) machines were developed. CNC technology enables computer operators to control, and instantly modify, not only the immediate task but also the feed rate, velocity, positioning, tolerances, location, and speeds of machines used for production.[29] In the late 1970s, the automotive industry pioneered the use of giant programmable robots that have multiple "arms" and "hands" and are able to perform multiple assembly operations.[30]

Today, robots are operated by AI. AI-enabled robots can "learn" new tasks in ways their predecessors could not. "Deep reinforcement learning" occurs when a robot is given instructions for a desired outcome and then uses trial and error to find a solution.[31] Moreover, robots can use "distributed machine learning"—in which multiple computers learn together and share this learning with each other—to learn from one another, so that eight arms working together for an hour can "learn" what one arm could learn in eight hours, and then can instantly share that knowledge with all the other robots on the factory floor.[32] This represents a new and qualitative leap in the mechanization of production.

---

https://www.forbes.com/sites/stevebanker/2019/01/01/20-things-to-know-about-artificial-intelligence-for-supply-chain-management/#5cac117d5371 [https://perma.cc/Q825–6F9C].

25. *See infra* Part I.B.

26. *AI-Spy*, *supra* note 6.

27. *AI Providers Will Increasingly Compete with Management Consultancies*, THE ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/ai-providers-will-increasingly-compete-with-management-consultancies [https://perma.cc/NN4T-MVJA**]**.

28. DAUGHERTY & WILSON, *supra* note 5, at 23.

29. *See generally* DAVID F. NOBLE, FORCES OF PRODUCTION: A SOCIAL HISTORY OF INDUSTRIAL AUTOMATION (1984).

30. For an overview of the concise history of industrial robots see generally A. Gasparetto, L. Scalera, *A Brief History of Industrial Robotics in the 20th Century,* 8 ADVANCES IN HISTORICAL STUDIES 1 (2019).

31. DAUGHERTY & WILSON, *supra* note 5, at 49.

32. *Id*. at 50.

c. Computer Vision, Amplification, and Speech Recognition

Computer vision "teach[es] computers to identify, categorize, and understand the content within images and video, mimicking and extending what the human visual system does."[33] Now-familiar examples include programs that enable autonomous cars to distinguish pedestrians from inanimate objects or to recognize wildlife that might dart onto the road and create a hazard. Computer vision also, as described above, enables factory robots to detect human workers and avoid injuring them.

AI can amplify human workers' sensory and analytical abilities, allowing them to do things they otherwise could not. For example, Autodesk's Dreamcatcher software uses next-generation computer-assisted design algorithms to create alternative design options based on specified parameters such as functional requirements, material type, manufacturing method, performance criteria, and cost restrictions.[34] Upskill's augmented reality program, Skylight, uses smart glasses to visually overlay precise instructions over a worker's natural field of vision, significantly reducing training time and mistakes.[35] Applications include jobs in field service (such as servicing wind turbines), manufacturing (such as wiring the electrical systems in airplanes), and materials handling (such as picking and kitting in warehouses).[36]

Just as AI is enabling computers to "learn" from "visual" inputs, it is also progressing rapidly in speech and audio recognition. Computers can be used to analyze audio signals in high-noise environments such as factory floors.[37] They are becoming increasingly adept at recognizing speech and converting it to text, translating words into different languages, and using verbal commands to control other machines or devices.[38] Some supporters of AI predict that AI will be able to use audio and video inputs to analyze a person's honesty, sentiment, and personality.[39] As described below, AI is increasingly being deployed in this way to conduct job interviews.[40] Thus, the enhanced ability of computers to learn, analyze, and augment humans' natural abilities is increasingly being used to manage the workforce, as the next section demonstrates.

---

33. *Id*. at 115–16.

34. *See Project Dreamcatcher*, AUTODESK RESEARCH, https://autodeskresearch.com/projects/dreamcatcher) [https://perma.cc/YGJ2–5DTE] (last visited Oct. 16, 2019).

35. *See How Skylight Works*, UPSKILL, https://upskill.io/skylight/how-it-works/ [https://perma.cc/NZ8Z-29HG] (last visited Oct. 16, 2019).

36. *See Augmented Reality for Material Handling*, UPSKILL, https://upskill.io/skylight/functions/material-handling/ [https://perma.cc/2DDS-PLBZ] (last visited Oct. 16, 2019).

37. DAUGHERTY & WILSON, *supra* note 5, at 64.

38. *Id*.

39. *See infra* Part I.B.1.b(ii).

40. *See infra* Part I.B.1.

B. AI in the Workplace

AI increasingly permeates HR practices in the workplace. Termed "People Analytics," AI is used to guide HR decisions for many areas, including making hiring decisions, monitoring performance, predicting an individual's work trajectory, evaluating workers to set compensation, and determining an employee's likelihood of terminating the employment relationship. Although the use of AI in the workplace is exploding, there is no precise data on its extent. Anecdotally, in the last five years, AI vendor booths at HR conventions have gone from zero to thirty to forty.[41] Moreover, most major business and management schools have held conferences and instituted classes on the subject of People Analytics.[42]

Below we describe some of the ways AI is being used, or is likely to be used in the near future, in the workplace. Each application of AI is fraught with legal implications, which will be explored subsequently in Part II.

1. Hiring

a. Recruiting and Sorting Applicants

Johnson & Johnson, a consumer products company, receives 1.2 million applications each year for 25,000 open positions, a ratio of nearly 50:1,[43] and it is hardly alone.[44] AI systems, like the one provided by talent-acquisition company HiredScore,[45] use keyword searches to scan and sort applications much faster than a human can.[46] Even if an applicant is unqualified for the particular job for which she has applied, that applicant may be a perfect fit for a different job at the same company. AI systems can redirect applicants to openings for which the applicant might be a better fit, or keep the application "on file" and notify the applicant when a suitable job later becomes available.[47] HiredScore maintains a database of applicants and, when a vacancy opens, automatically creates a shortlist of previous

41. *See, e.g.*, The vendor list at the 2019 convention for the Society of Human Resources Management. Exhibitors, Society for Human Resource Management—Annual Conference and Exposition (Jun. 23–26, 2019), https://expocad.shrm.org/Ann2019/ec/forms/attendee/index5.aspx#fpPanel [https://perma.cc/T44A-QZ3L].

42. *See, e.g.*, Wharton People Analytics Conference, The Wharton School, University of Pennsylvania (Apr. 2–3, 2020), https://wpa.wharton.upenn.edu/conference/ [https://perma.cc/4P74-VMBE] (an annual conference at Wharton Business School); Jeffrey Polzer, *Reimagining Management through People Analytics*, Harvard Bus. Sch. Dig. Initiative, (2017), https://digital.hbs.edu/data-and-analysis/di-talk-reimagining-management-people-analytics/ [https://perma.cc/SGW7-GBPP].

43. *Hire Education, supra* note 6.

44. *See* David D. Savage & Richard Bales, *Video Games in Job Interviews: Using Algorithms to Minimize Discrimination and Unconscious Bias*, 32 ABA J. LAB. & EMP. L. 211, 215 nn. 37–42 (2017).

45. *See* HIREDSCORE, https://hiredscore.com/ [https://perma.cc/T2PV-NG8V] (last visited Oct. 16, 2019).

46. *Hire Education*, *supra* note 6.

47. *Id*.

applicants who would be a good fit for the new opening.[48] Kronos Software uses algorithms to recruit, screen, track, hire, and complete employee verification of applicants.[49]

AI systems are designed to "look" beyond an applicant's resume and cover letter to discern patterns that might predict performance. For example, the technology and gaming company Nvidia has created an in-house applicant-tracking software package, which found that applicants submitting particularly long resumes tend to underperform on the job compared to their more concise peers.[50] Other AI investigations might identify other measurable factors that correlate with job tenure, employee attitude, upward advancement, disciplinary record, or personality fit with the company.[51] The use of such technology to attract, test, sort, and (as discussed immediately below) evaluate applicants raises a host of possible discrimination, privacy, and antitrust issues.[52]

b. Interviewing and Evaluating Applicants

Most HR professionals acknowledge that application forms and job interviews alone are not particularly effective methods of evaluating job candidates because the persons responsible for gathering and interpreting information may have poor judgement or individual preferences that do not align with company objectives.[53] Hence, HR professionals believe that data analytics can usefully augment the pool of information and produce better results, often by eliminating various forms of bias.[54] Data analytics incorporates AI in its use of three different sources of information: job tests, video-recorded interviews, and videogames.

(i) Job Tests

Paper-and-pencil or, more often today, online tests for measuring job-skill aptitude or personality have existed for decades. So long as they don't

48. *Id*.

49. *See Talent Acquisition*, KRONOS, https://www.kronos.com/products/talent-acquisition [https://perma.cc/6AVL-HTX7] (last visited Oct. 16, 2019); *see also* Harris Mateen, Book Note, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, 39 BERKELEY J. EMP. & LAB. L. 285 (2018).

50. *Hire Education*, *supra* note 6.

51. For a discussion of how recruiters, armed with AI, have developed ways to go beyond fine tune and widen searches for job candidates, see Noam Schieber, *A.I. as Talent Scout: Unorthodox Hires, and Maybe Lower Pay*, N. Y. TIMES (Dec. 6, 2018), https://www.nytimes.com/2018/12/06/business/economy/artificial-intelligence-hiring.html [https://perma.cc/V6SV-NDEC].

52. *See infra* Parts I.B.1, II.C.

53. *See* Mitchell Hoffman et al., *Discretion in Hiring*, [133, ISSUE 2] Q.J. ECON. 765, 765 (2018).

54. *Id*.; *see also* Josh Bersin, *Big Data in Human Resources: Talent Analytics (People Analytics) Comes of Age*, FORBES (Feb. 17, 2013, 8:00 PM), https://www.forbes.com/sites/joshbersin/2013/02/17/bigdata-in-human-resources-talent-analytics-comes-of-age/#7a2dc5dd4cd0 [https://perma.cc/J5CR-AJ5M].

ask personal questions or reflect discernibly biased assumptions, such tests are relatively uncontroversial.[55] What's new today, however, is the ability of AI to match applicants' scores on such tests—or even their answers to particular questions—to their job performance down the road, and then to use the resulting data to predict the performance of other future applicants.[56]

Labor economists Mitchell Hoffman, Lisa Kahn, and Danielle Li studied hiring at fifteen companies that employed workers in the same low-skilled service sector.[57] They compared companies that relied primarily on testing and data analytics with those that simply relied on job interviews. They found that:

> cohorts of workers hired with job testing have substantially longer tenures than cohorts of workers hired without testing, holding constant a variety of time-varying location and random variables. In our setting, job tenure is a key measure of quality because turnover is costly and workers already spend a substantial fraction of their tenure in paid training. This finding suggests that this job test contains useful information about the quality of candidates.[58]

Specifically, their study found that managers who relied primarily on objective test results achieved a fifteen percent increase in tenure as compared to the managers who did not.[59] When discretion was removed entirely and hiring corresponded exclusively to the test results, tenure increased further.[60] They conclude from this that "[o]ur results are broadly aligned with findings in psychology and behavioral economics that emphasize the potential of machine-based algorithms to mitigate errors and biases in human judgement across a variety of domains."[61]

(ii) Video-recorded Interviews

Pre-hire video-recorded interviews recently have become a tool in the recruiter's toolbox.[62] In pre-hire video interviews, applicants are asked questions specifically tailored to the particular open position.[63] Candidates digitally video-record their answers, usually online from home or their current office, using their desktop or laptop computer. The video is then transmitted to a company such as HireVue[64] that uses AI to analyze the video. HireVue uses AI to analyze the applicant's language patterns, verbal skills,

55. *See generally* Greenawalt v. Indiana Dep't of Corrections, 397 F.3d 587 (7th Cir. 2005).

56. *See* Mateen, *supra* note 49.

57. *See supra* note 53 at 765.

58. *Id.* at 766.

59. *Id*. at 769.

60. *See*, *e.g.*, *id*. at 766.

61. *Id.* at 769.

62. *See* DAUGHERTY & WILSON, *supra* note 5, at 51; *How an Algorithm May Decide Your Career*, THE ECONOMIST (Jun. 21, 2018), https://www.economist.com/business/2018/06/21/how-an-algorithm-may-decide-your-career [https://perma.cc/QPG2-YRTZ]; *See also Hire Education, supra* note 6.

63. DAUGHERTY & WILSON, *supra* note 5, at 51.

64 HIREVUE, https://www.hirevue.com/ [https://perma.cc/7W9Q-MDB9] (last visited Oct. 16, 2019).

and emotions[65] by, for example, identifying facial expressions, intonation, gestures, and word choice.[66] It then uses its machine learning algorithms to evaluate the candidates' work styles, predict their ability to work with others, and assess general cognitive ability. It uses this information to prioritize applicants.[67] HireVue claims to provide such services for over 700 companies,[68] including Intel,[69] Accenture,[70] and Unilever.[71] Another company that offers services similar to HireVue's is Cognisess, which promises to use video analytics to identify microexpressions that reveal a candidate's emotions and motivations.[72]

Although employers have used job interviews for centuries to evaluate an applicant's personality and cognitive ability on the basis of their body language and word choice, video-recorded interviews make it possible to for interview data to be stored and analyzed indefinitely. The questions asked in a video-recorded interview may be indistinguishable from the types of questions asked in a typical job interview, at least for now. However, HireVue's most significant ability to add value to the job-application process will come down the road, after it has tracked the success or failure of the applicants its clients have hired and used AI to correlate the interview idiosyncrasies of millions of video-recorded applicants with their success or failure on the job. HireVue could then use the resulting data to predict the performance of new applicants.

(iii) Video Games[73]

AI and video games can be used together to screen and sort applicants.[74] Video games are sometimes used at the early stage of the search process.[75]

65. *Pre-Employment Assessments*, HIREVUE, https://www.hirevue.com/products/assessments/pre-employment-video-assessments [https://perma.cc/4CST-XTHG] (last visited Oct. 16, 2019).

66. *See Hiring Education*, *supra* note 6; *How an Algorithm May Decide Your Career*, *supra* note 62 (explaining that successful applicants maintain eye contact with the camera throughout the interview, sound confident, sit up straight, and avoid thrashing gesticulation)

67. HIREVUE, *supra* note 64.

68. *HireVue Video Interviewing Software*, HIREVUE, https://www.hirevue.com/products/video-interviewing/ondemand [https://perma.cc/643T-L4HU] (last visited Nov. 5, 2019) .

69. *Id*.

70. *Hire Education*, *supra* note 6.

71. DAUGHERTY & WILSON, *supra* note 5, at 51.

72. *See* Cognisess, *A Guide to Video Analytics*, YOUTUBE (Apr. 26, 2018), https://www.cognisess.com/video-analytics/**;** https://www.youtube.com/watch?v=6U56S6eV3Pg (describing Cognisess' software platform) [https://perma.cc/QY7N-X4NU].

73. Portions of this section have been taken from Savage & Bales, *supra* note 44. For a comprehensive discussion of using video games in the applicant-screening process, and the legal implications of the same, see *id.*

74. *See* DAUGHERTY & WILSON, *supra* note 5, at 51; *Hire Education*, *supra* note 6.

75. *Hire Education*, *supra* note 6.

Companies such as Knack,[76] Deloitte,[77] Pymetrics,[78] and HireVue[79] (through its acquisition of MindX) have applicants play a video game for about twenty minutes, then use the resulting data to analyze the applicants' risk appetites, mental agility, persistence,[80] and ability to read emotional versus contextual clues.[81] For example, "Wasabi Waiter", designed by Knack, places the job applicant in the role of a server at a sushi restaurant who must figure out which dishes to recommend to customers. The designer of the game, Guy Halfteck, explains:

> The player has to engage in multiple micro-decisions, think about prioritizing, about [the] sequence of taking actions, about persisting when the game becomes more challenging . . . The game collects all the data points about the entirety of the behavior during the game . . . Then we analyze that data to extract insight into the intellectual and personal makeup of that person.[82]

Even one law firm is getting in on the action: in late 2018, O'Melveny & Myers began using cognitive-testing video games to assess law students for legal employment.[83] Using video games in hiring raises legal concerns involving the possibility of subtle discrimination; this is explored below.

2. Performance, Pay, & Promotions

After a company uses AI to hire an employee, it may use AI to track performance, determine pay, and make decisions about promotions and/or dismissal. For example, the data management company Workday[84] provides a comprehensive "people analytics" product to analyze workforce demographics, monitor turnover trends, and track performance.[85] According

---

76. KNACKAPP, https://www.knack.it/ [https://perma.cc/F9YJ-7ZJ5] (last visited Nov. 8, 2019).

77. Rob Davies, *Everything to Play for as Employers Turn to Video Games in Recruitment Drive*, THE GUARDIAN (Nov. 28, 2015, 11:00 AM), https://www.theguardian.com/money/2015/nov/28/psychometric-tests-games-recruitment-interview [https://perma.cc/WD3Y-PZVB].

78. *Employers*, PYMETRICS, https://www.pymetrics.com/employers/ [https://perma.cc/L9ZD-QF6H] (last visited Nov. 8, 2019).

79. Dan Parker, *7 Things You Need to Know About Game-Based Cognitive Assessments*, HIREVUE (Jul. 12, 2018), https://www.hirevue.com/blog/7-things-you-need-to-know-about-game-based-cognitive-assessments [https://perma.cc/46W9-PR4J]

80. Davies, *supra* note 77.

81. DAUGHERTY & WILSON, *supra* note 5, at 51.

82. *Could Video Games Be the Next Job Interview?*, NATIONAL PUBLIC RADIO: ALL TECH CONSIDERED (Dec. 1, 2013, 8:13 AM), http://www.npr.org/sections/alltechconsidered/2013/12/01/246999632/playing-the-game-to-get-the-job [https://perma.cc/57NK-N6JJ].

83. *O'Melveny Could Set Trend with Law Student Cognitive Testing*, BLOOMBERG LAW (Nov. 23, 2018, 3:01 AM), https://news.bloomberglaw.com/employee-benefits/omelveny-could-set-trend-with-law-student-cognitive-testing. Thanks to Laura Cooer for calling our attention to this news article.

84. *Reporting and Analytics*, WORKDAY, https://www.workday.com/en-us/applications/human-capital-management/people-analytics.html [https://perma.cc/LU7H-LCM] (last visited Nov. 10, 2019).

85. *Id*.

to its website, Workday boasts that it offers companies the ability to: "[m]ake better recruiting decisions with quality-of-hire metrics," "[g]et a complete view of your people and operations" and "detect patterns that you might not see or have time to discover."[86] Workday claims it can examine some sixty factors—such as time an employee takes between days off for vacations, changes in an individual's supervisor, and other seemingly innocuous considerations—to predict which employees are likely to quit, which ones are likely to be disgruntled, and how the employer might retain the best employees.[87]

Another company, Arena,[88] which focuses on the healthcare industry, uses information from job applications and third parties to predict which applicants are likely to stay for more than a year. Twine Labs[89] tracks "hundreds of variables" which it uses to recommend internal candidates for promotion.[90] Infosys is considering using AI to identify employees for raises based on their performance and their pay relative to peers.[91]

At companies using AI to perform employee assessment, the role of managers and supervisors is likely to change significantly. For example, technical supervision (ensuring that a worker is doing her job properly) and disciplinary supervision (ensuring that an employee is behaving appropriately in the workplace) may be performed by different supervisors, or may be divided among several supervisors using several sets of algorithms.[92] Moreover, the authority to give technical instruction may be delegated to individuals who are not employed by the same company or even in the same country.[93] Disaggregation and outsourcing will permit more specialized supervision and facilitate cross-company activities and standard-setting. However, they also can facilitate HR collusion and illegal

86. *Id.*

87. *Hire Education*, *supra* note 6.

88. ARENA, https://www.arenasolutions.com/ [https://perma.cc/9J7Z-ZF8S] (last visited Oct. 16, 2019).

89. TWINE, https://www.twinelabs.com/ [https://perma.cc/YC6Y-7HN6] (last visited Oct. 16, 2019).

90. Hire Education, *supra* note 6.

91. *Id*. On the other side of the spectrum are gig-economy companies like Uber that have effectively outsourced worker assessment to customers. *See User-rating Systems are Cut-rate Substitutes for a Skilful Boss*, THE ECONOMIST (Jun. 30, 2018), https://www.economist.com/finance-and-economics/2018/06/30/user-rating-systems-are-cut-rate-substitutes-for-a-skilful-boss [https://perma.cc/AXP9-DSB5]. These companies typically rely on a "star" system, where customers rate the worker on a scale of, for example, one to five. Five-star workers may get more work assignments; one-star workers may get "fired". Some scholars have argued that these rating systems can be tainted with bias. For example, if Muslim drivers receive consistently lower ratings than white drivers, Muslim drivers will be affected in very real and quantifiable ways. Customer rating systems, and the issues they raise, are not limited to gig-economy companies, as an increasing number of conventional companies are following suit. *See User-rating Systems*, *supra*.

92. *See* IBA, *supra* note 7, at 50–51.

93. *Id.*

blackballing, thereby generating potential antitrust and collusion concerns, which will be discussed below.

C. Electronic Surveillance

Data is the life blood of AI. Indeed, in the workplace, AI is inseparable from the technology used to collect data. AI algorithms are built from troves of data that a computer amasses, organizes, and analyzes to predict outcomes and achieve a stated goal. The goal of HR AI—or "people analytics," as it is often termed—is an efficient, safe, productive, and effective operation. AI uses historical data from one or more workplaces to set a baseline and identify patterns. It then uses data about ongoing operations to draw comparisons, identify deviations, and make predictions. Hence, employers need to collect data about their employees in order to develop, implement, and utilize AI. They do this by means of electronic monitoring and surveillance. However, current monitoring and surveillance technology has the potential to facilitate a massive intrusion into employee privacy inside and outside of the workplace, and raises a host of other legal concerns, which will be explored in Part II, below.[94] In this section, we describe some of the methods and capabilities of AI linked electronic surveillance.

1. New Types of Electronic Surveillance

Labor historians have extensively documented employers' use of company spies and thugs to identify and brutalize union organizers. One such example is the Ford Motor Company's use of its Sociology Department to invade workers' homes to forage for evidence of union activity.[95] Today, AI and electronic monitoring enable employers to engage in worker surveillance in ways that are arguably more effective.

Electronic surveillance and monitoring is ubiquitous, invisible, and perpetual. For example, the company Slack[96] uses AI to assess how quickly

94. In addition to the labor law issues discussed in this section, the use of AI in the workplace can also implicate discrimination, violations of privacy, collusion and black-listing, each of which are discussed in separate sections.

95. There is a vast literature about the use of spies and thugs by employers through the late 19th and 20th century to intimidate union supporters and prevent unionization. For some recent contributions, *see, e.g.*, ROBERT M. SMITH, FROM BLACKJACKS TO BRIEFCASES: A HISTORY OF COMMERCIALIZED STRIKEBREAKING AND UNION BUSTING IN THE UNITED STATES 75–97 (2003) (documenting extent of, and tactics of, spies and labor spy agencies by U.S. employers from the early 20th century); S. PAUL O'HARA, INVENTING THE PINKERTONS; OR, SPIES, SLEUTHS, MERCENARIES, AND THUGS (2016); *accord* STEPHEN H. NORWOOD, STRIKEBREAKING AND INTIMIDATION: MERCENARIES AND MASCULINITY IN TWENTIETH CENTURY AMERICA 175–178 (2002) (on use of 'plug uglies' and other thugs to spy on and intimidate pro-union workers in Ford Motor Company's River Rouge plant in the 1920s and 1930s); Michael Ballaban, *When Henry Ford's Benevolent Secret Police Ruled His Workers*, JALOPNIK (Mar. 23, 2014, 1:35 PM), https://jalopnik.com/when-henry-fords-benevolent-secret-police-ruled-his-wo-1549625731 [https://perma.cc/4NA5–76EL] (describing Ford's Sociology Department and its intrusions into the homes of Ford workers).

96. SLACK, https://slack.com/ [https://perma.cc/389U-NH64] (last visited Oct. 16, 2019).

workers accomplish each task and to monitor workers who might be dozing or misbehaving.[97] The company Cogito[98] uses AI to listen to customer-service calls and grade workers on empathy and how quickly and effectively they solve complaints.[99] Microsoft's MyAnalytics[100] amalgamates data from a worker's emails, calendars, and phones to calculate how the worker spends her time, how often she is in touch with key contacts, and whether she multitasks too frequently.[101] The company Veriato[102] has produced software that registers everything that happens on a worker's keyboard; it can flag poor productivity, misconduct (such as stealing company records), and negative attitudes.[103] The company KeenCorp[104] analyzes an employee's emails, focusing on word patterns and content, and then assigns each employee a number reflecting the employee's level of engagement: a high number indicates an employee feeling positive and engaged, a low number an employee feeling disengaged and expressing negative emotions.[105] The company Teramind[106] sends workers pop-up warnings if it suspects they are slacking or about to share confidential documents.[107] Some white collar workplaces have installed a system called OccupEye,[108] in which sensors on employees chairs indicate how often an employee is at her desk and how long

97. *AI-Spy*, *supra* note 6, at 13.

98. COGITO, http://www.cogitocorp.com/ [https://perma.cc/ X4QK-ZD66] (last visited Oct. 16, 2019).

99. *Id*.; *see also Customer Service Could Start Living Up to its Name*, THE ECONOMIST (March 28, 2018), https://www.economist.com/special-report/2018/03/28/customer-service-could-start-living-up-to-its-name [https://perma.cc/DCK7-WBDN].

100. *Microsoft MyAnalytics*, MICROSOFT, https://products.office.com/en-us/business/myanalytics-personal-analytics (last visited Oct. 16, 2019) [https://perma.cc/N3TA-H95C].

101. *There Will Be Little Privacy in the Workplace of the Future*, THE ECONOMIST (Mar. 31, 2018), https://www.economist.com/special-report/2018/03/28/there-will-be-little-privacy-in-the-workplace-of-the-future [https://perma.cc/Y9WX-XMTV].

102. VERIATO, https://www.veriato.com/ [https://perma.cc/WXK7-KAHD] (last visited Oct. 16, 2019).

103. *There Will Be Little Privacy*, *supra* note 101.

104. KEENCORP, http://www.keencorp.com/ [https://perma.cc/Q7QP-A7PE] (last visited Oct. 16, 2019).

105. Frank Partnoy, *The Secrets in Your Inbox*, THE ATLANTIC (Sept. 2018), https://www.theatlantic.com/magazine/archive/2018/09/the-secrets-in-your-inbox/565745/ [https://perma.cc/Y7DP-CW5V]. (noting that "heat maps", created by aggregating employees' engagement numbers by department or division, can ostensibly be used to flag when something has suddenly gone wrong in that department or division, such as noncompliance with government rules or sexual harassment).

106. TERAMIND, https://www.teramind.co [https://perma.cc/V3TR-LGR5] (last visited Oct. 16, 2019).

107. Miranda Katz, *The Creative Ways your Boss is Spying on You*, WIRED (Aug. 12, 2018, 7:00 AM), https://www.wired.com/story/the-creative-ways-your-boss-is-spying-on-you/ [https://perma.cc/3DTF-BCNG].

108. OCCUPEYE, https://www.occupeye.com (last visited Oct. 16, 2019) [https://perma.cc/7BQV-VFKH].

she is on breaks.[109] Many employers install GPS devices on employees' phones as well as vehicles that can track their employees' every movements, both on and off the job.[110]

Employers are beginning to require employees to don wearable tracking devices.[111] For example, Ultrasonic[112] wristbands issued by Amazon track workers' precise locations and hand movements, gauging workers' productivity and accuracy and vibrating to nudge workers into being more efficient.[113] Other employers require their employees to wear Fitbits that can monitor and provide employers with information about employees' heart rates, blood pressure, and sleep patterns.[114] In 2018, Amazon patented a "haptic wristband" that observes employees' every movement, including quirks, fidgets, and bathroom breaks.[115] Another electronic wristband measures employees' moods. "Smart glasses" improve peripheral or low light vision—but also enable an employer to see whatever an employee sees, as if looking through their eyes.[116] There are patents pending for biofeedback clothing, such as a vests and exoskeletons that monitor heart rates, stress levels, and other physiological and psychological states.[117] Some employers are requiring employees to wear caps and headbands that measure brain activity and detect fatigue levels.[118] IBM and Hyundai have utilized wearable technology such as bionic bodysuits and exoskeletons to enhance some

109. Ryan Derousseau , *The Tech That Tracks Your Movements at Work*, BBC Ryan Derousseau, *The Tech That Tracks Your Movements at Work*, BBC WORKLIFE (June 14, 2017), http://www.bbc.com/capital/story/20170613-the-tech-that-tracks-your-movements-at-work [https://perma.cc/9TRF-TA7X].

110. *See, e.g.*, Kaveh Waddell, *Why Bosses Can Track Their Employees 24/7*, THE ATLANTIC (Jan. 6, 2017), https://www.theatlantic.com/technology/archive/2017/01/employer-gps-tracking/512294/ [https://perma.cc/P3SZ-DYZU].

111. *See* Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology*, 63 ST. LOUIS U. L.J. 21, 34–41 (2019) (providing an overview of currently used and pending wearable surveillance devices).

112. *Katz*, *supra* note 107.

113. *AI-spy*, *supra* note 6; *There Will Be Little Privacy*, *supra* note 101.

114. *See, e.g.*, Suzanne McGee, *How Employers Tracking Your Health Can Cross The Line And Become Big Brother*, THE GUARDIAN (May 1, 2015, 8:30 AM), https://www.theguardian.com/lifeandstyle/us-money-blog/2015/may/01/employers-tracking-health-fitbit-apple-watch-big-brother [https://perma.cc/95G2–7U63].

115. Ajunwa, *supra* note 111, at 34; *see also* Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)*, N. Y. TIMES (Feb. 1, 2018) https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html [https://perma.cc/2TLS-P4WL].

116. *See* Ajunwa, *supra* note 111, at 25–26; *see also 9 Ways Smart Glasses Can Increase Employee Productivity: Boost Workplace Performance With Augmented Reality*, FLOAT, https://gowithfloat.com/2015/04/9-ways-smart-glasses-can-increase-employee-productivity/ [https://perma.cc/D3QK-B3N7] (last visited Nov. 10th, 2019).

117. *See* Ajunwa, *supra* note 111, at 39–41.

118. *Id*. at 38–40.

employees' strength[119] and guide their movements—garb that also provides employers with detailed information about employees' biological, physiological, and emotional conditions.[120]

Companies have also updated the classic employee badge into a monitoring device. The company Humanyze[121] requires its employees to wear an ID badge containing a microphone that records conversations, a Bluetooth and infrared sensor that monitors where they are (how long do they spend in the break room? Outside the building smoking?), and an accelerometer that notes when they move.[122] The company's software collects data on how much time each worker spends with talking with people and the proportion of time spent speaking versus listening.[123] According to Richard Reice, writing for Bloomberg Law:

> [Humanyze's] employee ID badges . . . incorporate biometric measuring capabilities that track movements and interactions in the office, including the length of conversations and voice tones via built-in microphones. Referred to as "people analytics," [Humanyze boasts that] these devices can help companies understand how their employees interact and move about the office which, among other things, can lead to a better-designed workplace, adjustment of module workplaces around project teams, or—more simply—identification of "risky" behavior.[124]

In a similar vein, Hitachi has created the "Business Microscope," a device affixed to a lanyard that serves as a security badge and key but also enables the company to know which workers are interacting with which others by means of a signal sent when two badge-wearing people are in proximity.[125] This technology tells the company how often a worker talks to coworkers, how energetic and animated the conversation is, and whether the employee is an active participant in meetings or group conversations.[126] Presumably the technology also has the capacity to record, and store, actual conversations.[127]

---

119. Richard M. Reice, *Wearables in the Workplace—A New Frontier*, BLOOMBERG LAW (May 24, 2018, 3:40 AM), https://news.bloomberglaw.com/daily-labor-report/wearables-in-the-workplacea-new-frontier [https://perma.cc/2D2T-RMUA].

120. Ajunwa, *supra* note 111, at 39–41.

121. HUMANYZE, https://www.humanyze.com/ [https://perma.cc/F4HN-QL8M] (last visited Oct. 16, 2019).

122. *See There Will Be Little Privacy*, *supra* note 101.

123. *Id*.

124. Reice, *supra* note 119.

125. *See, e.g.*, *'Business Microscope' to Track Employees' Every Move at Workplace*, THE HINDU BUSINESS LINE (Mar. 10, 2018), https://www.thehindubusinessline.com/news/business-microscope-to-track-employees-every-move-at-workplace/article20723763.ece [https://perma.cc/2ZJH-A962].

126. *Id*.

127. For a description of these and other emergent wearable monitoring technologies, see Ajunwa, *supra* note 111.

One new frontier in the burgeoning field of people analytics is monitoring workers' emotional states and shaping their behaviors.[128] An MIT research team headed by finance professor Andrew Lo concluded, on the basis of simulated experiments, that emotionally stable and resilient workers perform better in stressful situations than those who are easily riled. As a result, they are developing wearable wristwatches and badges that have sensors to monitor workers' emotional states. [129] Several banks and brokerage firms have adopted these devices.[130]

Perhaps the most insidious monitoring technology is Radio Frequency Identification (RFID). RFID allows employers to track microchips attached to workers and goods using radio waves. It can also be implanted under employees' skin for identification and access to facilities. For example, Swedish company Biohax International makes an implantable RFID chip housed inside a bioglass capsule smaller than a gel aspirin tab, which is injected into the web of an employee's skin between their thumb and forefinger. The capsule uses near-field communication (NFC) to communicate with enabled devices.[131] RFID is touted for its efficiency-enhancing properties. As one commentator explains, "Once the capsule is injected, an employee need only place his or her hand in near proximity to an NFC-enabled door, computer, vending machine, photocopier, or other device to gain entry, record a purchase, or authorize access."[132] RFID can also be used to give employers ongoing information about workers' location, conversations, physiological state, psychological condition, and more.[133]

To be sure, some AI-enabled monitoring is benign or even constructive. Computer vision enhanced with AI can ensure workers do not enter dangerous work areas without safety equipment like hard hats and gloves and can monitor the factory floor for signs of danger.[134] Wearable vests and "exoskeletons" can enable workers to perform arduous physical tasks more safely. For example, Ekso Works Industrial Exoskeleton, created by Ekso

---

128. For examples of how electronic wearable technology can be used to monitor employee emotional states and alter employee decisions and behavior, see Timothy L. Fort et al., *The Angel on Your Shoulder Prompting Employees To Do The Right Thing Through The Use Of Wearables,* 14 NW. J. TECH. & INTEL. PROP. 139, 148–153 (2016).

129. Thomas Heath, *This Employee ID Badge Monitors and Listens to You At Work—Except in the Bathroom*, WASH. POST (Sept. 7, 2016, 8:33 AM), https://www.washingtonpost.com/news/business/wp/2016/09/07/this-employee-badge-knows-not-only-where-you-are-but-whether-you-are-talking-to-your-co-workers/ [https://perma.cc/KUG5–5TY6].

130. Hugh Son, *Wall Street's Next Frontier Is Hacking Into Emotions of Traders*, BLOOMBERG BUSINESSWEEK (Sept. 1, 2016, 2:00 AM), https://www.bloomberg.com/news/articles/2016–09–01/wall-street-s-next-frontier-is-hacking-into-emotions-of-traders [https://perma.cc/8U5X-SHG9].

131. Reice, *supra* note 119.

132. *Id*.

133. For an example of one of the many companies providing such products, see *Employee Tracking & Visitor Monitoring System from Long Range*, LITUMIOT, https://litumiot.com/employee-people-tracking/ [https://perma.cc/8ZAM-PZFZ].

134. *See There Will Be Little Privacy*, *supra* note 102; AI-spy, *supra* note 6.

Bionics, is a bionic suit that enables the wearer to lift heavy tools as if they weightd nothing at all.[135] Similar devices enable workers with restricted mobility to perform heavy lifting.[136] However, as described below, many aspects of AI-enabled workplace monitoring threaten to suppress opposition, punish union supporters, and otherwise undermine workers' rights.[137]

2. Monitoring Off-Work Activity

In addition to monitoring on-duty conduct, AI enables employers to monitor of off-duty (particularly online) conduct continuously and extensively. Today, employers typically review an applicant's publicly available social media accounts before a hiring decision is made[138] to determine whether the applicant's social media history should disqualify her from being hired.[139] Current employees often are fired for inappropriate social media posts or tweets.[140] So far, such firings do not usually result from an employer's pervasive monitoring of employees' social media accounts,[141] but instead from a "friend" or co-worker alerting management about the offensive posts or tweets of fellow employees.[142] This is because few employers have the time or inclination to pervasively monitor their employees' social media accounts. However, emerging AI applications that can engage in wide, perpetual sweeps of social media will change the frequency and penetration of employer social media eavesdropping. Companies now can use AI to comprehensively monitor an employee's on-duty work communications and off-duty social media communications.[143]

---

135. *See EksoWorks*, EKSO BIONICS, https://eksobionics.com/eksoworks/ [https://perma.cc/T6W8–4FAF].

136. Ajunwa, *supra* note 111, at 28 (citing Adam Rogers, *We Try a New Exoskeleton for Construction Workers*, WIRED (Apr. 28, 2015, 7:00 AM), https://www.wired.com/2015/04/try-new-exoskeleton-construction-workers/ [https://perma.cc/624V-HYLA]).

137. *See infra* Part II.D.

138. *See* Kathleen M. Hidy & Mary S. E. McDonald, *Risky Business: The Implications of Social Media's Increasing Role in Employment Decisions*, 18 J. LEGAL STUD. IN BUS. 69 (2013); Tommy Katsabian, *Employees' Privacy in the Internet Age: Towards a New Procedural Approach*, 40 BERKELEY J. EMP. & LAB. L. 203, 215 (2019).

139. *See* Terry M. Dworkin, *Protecting Private Employees from Enhanced Monitoring: Legislative Approaches,* 28 AM. BUS. L.J. 59, 75 (1990); Don Mayer, *Workplace Privacy and the Fourth Amendment: An End to Reasonable Expectations?,* 29 AM. BUS. L.J. 625, 626 (1991).

140. *See* Dworkin, *supra* note 139, at 71–73.

141. A handful of employers have attempted to require applicants or employees to provide the employer with their social-media media passwords. *See* Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 J. HIGH TECH. L.J. 42 (2014). However, this does not appear to be the norm.

142. Ruth Mantell, *Your Social-Media Posts Could Get You in Hot Water*, MARKETWATCH (Jun. 6, 2012, 11:44 AM), http://articles.marketwatch.com/2012–06–04/finance/31951218_1_facebook-page-social-media-policiesworkers [https://perma.cc/88KH-NDH7].

143. For an example, Fama Technologies, Inc. uses artificial intelligence to comprehensively scan the public web and online social media to detect troubling images and to flag words that might indicate a propensity for harassment, bigotry, or undesirable behavior. *See Social Media Background Check*, FAMA, https://www.fama.io/social-media-background-checks-a2 [https://perma.cc/64VC-ZDTQ].

Employers have some legitimate reasons to use AI to monitor employees' off-duty and on-line conduct. Racist or sexist posts may indicate a proclivity to racist or sexist conduct or harassment in the workplace. Aggressive posts may indicate a bullying personality. A post containing the company's name and words or phrases like "gun" or shoot" or "blow up" could be a red flag for impending workplace violence. Posts indicating illegal drug use or overconsumption of alcohol could raise workplace safety concerns. Posts disparaging the company or its products could harm the company's reputation. Indeed, the ease of conducting such monitoring using AI technology, coupled with the potential liability for wrongful hiring[144] or retention or failing to prevent harassment or violence, may begin to nudge more and more employers to comprehensively monitor their employees' social media accounts.[145] The more they do, however, the more serious the privacy concerns become.

3. Data Retention and Use

Technology not only creates the potential for highly intrusive monitoring, but also raises questions about how employers will use the data they collect about employees' performance, with whom they will share it, and how long they will keep it. AI-enhanced data collection, retention, and analytic capabilities threaten to create a permanent record of employee productivity, activity, and medical and physiological attributes. Some companies claim that AI-amassed data will be collected only in the aggregate, rather than on individual workers, in order to provide dashboard analytics that enable managers to monitor the performance of groups and divisions.[146] In Europe, data protection laws restrict the collection of individualized data.[147] However, there are no comparable restrictions in the US, and services offered by companies such as Workday, Arena, and Twine Labs indicate they already are collecting and using individualized assessment data.[148] Below we discuss the discrimination, privacy, antitrust, and labor law issues that can arise from today's data collection and retention practices.[149]

144. LEX K. LARSON, 1 EMPLOYMENT SCREENING § 10-2.3 (2006) (defining negligent hiring).

145. Partnoy, *supra* note 105 (arguing that the same types of potential liability may encourage employers to increase their use of text analytics to monitor employees' workplace emails).

146. *See* IBA, *supra* note 7, at 102; *There Will Be Little Privacy*, *supra* note 101.

147. *See infra* note 209 and accompanying text.

148. *See supra* notes 97-112 and accompanying text [first two paragraphs of this section].

149. *See infra* Parts II.B and II.C.

III. LEGAL ISSUES STEMMING FROM AI IN THE WORKPLACE

A. Employment Discrimination

Several legal scholars have warned about the danger of AI entrenching discrimination and bias into firm-level HR practices. They argue that AI can amplify or mask discriminatory prejudices and disproportionately exclude underrepresented groups of workers. [150] Defenders of the use of AI in HR, on the other hand, argue that it has the potential to reduce discrimination by minimizing or eliminating human judgment, and by identifying hiring practices that are unintentionally exclusionary.[151] While both effects are plausible, it is clear, at the least, that the use of AI in the workplace raises serious concerns that as of yet are largely unaddressed by existing anti-discrimination law.

AI can operate at several stages in the work relationship, including hiring, wage setting, evaluation, promotion, discipline, and dismissal. If algorithms are constructed that embody insidious racial or gender stereotypes, then women or people of color will be seriously disadvantaged in the labor market. The same would occur from the use of stereotypes concerning age, disability, religion, or other protected classes. Yet if it is an algorithm that is producing the discriminatory outcome, rather than a human decision maker, it may be nearly impossible for the worker who is adversely affected to mount a successful legal challenge.

1. How AI Can Generate Bias

There are numerous ways in which AI can introduce bias into the hiring, evaluation, compensation, and disciplinary processes. First, as the oft-observed maxim states, with computer programs, it is "garbage in, garbage out." Similarly, with algorithms, it is "bias in, bias out."[152] If the individuals providing the search criteria or input data, or the programmers creating the algorithm, are themselves biased, that bias could easily infect the algorithm. The output likely will then reflect (or even amplify) the same bias. For example, algorithms analyzing video-recorded interviews might disproportionately disadvantage certain groups of applicants based on race,

150. *See*, *e.g.*, Jennifer Alsever, *Is Software Better at Managing People Than You Are?*, FORTUNE (Mar. 21, 2016, 9:00 AM), http://fortune.com/2016/03/21/software-algorithms-hiring/ [https://perma.cc/LJ4T-TMQ7]; Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016); Allan G. King & Marko J. Mrkonich, *"Big Data" and the Risk of Employment Discrimination*, 68 OKLA. L. REV. 555 (2016); Kevin McGowan, *Big Bad Data May Be Triggering Discrimination*, BLOOMBERG LAW (Aug. 15, 2016), https://bol.bna.com/big-bad-data-may-be-triggering-discrimination/; Dustin Volz, *Silicon Valley Thinks It Has the Answer to Its Diversity Problem*, THE ATLANTIC (Sept. 26, 2014), http://www.theatlantic.com/politics/archive/2014/09/silicon-valley-thinks-it-has-the-answer-to-its-diversity-problem/431334/ [https://perma.cc/5UJ5-LL36].

151. *See*, *e.g.*, Savage & Bales, *supra* note 44, at 213–14.

152. DAUGHERTY & WILSON, *supra* note 5, at 121; *see also* Charles A. Sullivan, *Employing AI*, 63 VILL. L. REV. 395 (2018).

ethnicity, geographic origin, or socio-economic background by flagging certain culturally specific voice intonations, speech patterns, or hand gestures.

More subtly, the creators of algorithms tend to rely on an employer's past hiring data to build predictive formulas.[153] Companies want to replicate their best workers, so they will use algorithms that statistically match job applicants with these workers. If a company does not have a history of hiring a certain class or classification of individuals, the algorithms that are built using past hiring data will systematically exclude these individuals from consideration for future open positions. For example, if a fire department is comprised almost exclusively of men, past hiring data might emphasize the importance of physical prowess relative to endurance. Likewise, Silicon Valley has long been criticized for its white-male-dominated workplaces;[154] a hiring algorithm based on current workplace demographics likely will replicate and entrench past hiring practices.[155] Similarly, using AI in hiring can result in "classification bias," which Pauline Kim defines as "the use of classification schemes that have the effect of exacerbating inequality or disadvantage along the lines of race, sex or other protected category."[156] For example, many online platforms, such as Facebook, permit advertisers—and job recruiters—to target a demographically restricted audience based on their interests, preferences, and characteristics, including age, sex, ethnicity, and race.[157] Though this type of algorithmic bias is usually treated as under a theory of disparate impact, Stephanie Bornstein has argued that if the model "best worker" upon which an algorithm is predicated is based on discriminatory stereotypes (such as the stereotypes at issue in *Price Waterhouse v. Hopkins*[158]), the resulting algorithm could give rise to a theory of disparate treatment discrimination.[159]

Moreover, using AI in hiring can replicate or amplify real prejudices that already exist in society.[160] For example, a study by Latanya Sweeney, former chief technology officer for the United States Federal Trade Commission, found that when a Google search is performed on a person's name, Google

153. Much of this paragraph is taken from Savage & Bales, *supra* note 44, at 218.

154. Stacy Jones & Jaclyn Trop, *See How the Big Tech Companies Compare on Employee Diversity*, FORTUNE (July 30, 2015, 9:00 AM), http://fortune.com/2015/07/30/tech-companies-diveristy/ [https://perma.cc/N538-PXR4].

155. Saul Hansell, *Google Answer to Filling Jobs Is an Algorithm*, N.Y. TIMES (Jan. 3, 2007), http://www.nytimes.com/2007/01/03/technology/03google.html?_r=1. [https://perma.cc/4DAC-KFC5].

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

157. Pauline T. Kim & Sharion Scott, *Discrimination in Online Employment Recruiting*, 63 ST. LOUIS U. L.J. 1 (2019).

158. Price Waterhouse v. Hopkins, 490 U.S. 228 (1989).

159. Stephanie Bornstein, *Antidiscriminatory Algorithms*, 70 ALA. L. REV. 519 (2018).

160. Pauline T. Kim, *Auditing Algorithms for Discrimination*, 166 U. PA. L. REV. ONLINE 189 (2017) ("*Auditing Algorithms*") (noting that "[e]ven the most carefully designed systems may inadvertently encode preexisting prejudices or reflect structural bias.").

AdSense is much more likely to generate ads that suggest an arrest record for persons with typical African-American names (DeShawn, Darnell, Jermaine) than for those with typical non-Hispanic white names (Geoffrey, Jill, Emma).[161] The mere suggestion of the possibility of an arrest record, even if no such record exists, could subconsciously persuade a hiring manager to choose the "less risky" candidate.[162]

Moreover, algorithms that adopt facially neutral criteria can nonetheless create bias in operation. For example, in one study, business school professors Anja Lambrecht and Catherine Tucker placed ads for jobs in STEM (science, technology, engineering, and math) subjects.[163] They found that Facebook was significantly more likely to show such ads to men than to women. This was not because of conscious bias on the part of Facebook algorithm writers. It occurred because women, who control a high proportion of household spending, are a more valuable demographic than men,[164] making ads targeting women more expensive. As a result, the algorithm targeted the ads toward men, where the return on investment would be higher. They conclude that "[a]n algorithm which simply optimizes cost-effectiveness in ad delivery will deliver ads that were intended to be gender-neutral in an apparently discriminatory way, due to crowding out.[165]

A recent article in Reuters showed how AI can create bias in the hiring process even when no individual decision maker is operating from covert or implicit bias.[166] The researchers studied a hiring spree by Amazon in 2015, when it announced plans to increase its workforce by more than 50,000 people nation-wide. To do this, Amazon developed an algorithm to screen the avalanche of resumes it anticipated receiving. The algorithm was based on patterns observed in previous hiring over the previous ten years, a baseline during which the company's hiring was overwhelmingly male. As a result, "Amazon's system taught itself that male candidates were preferable. It penalized resumes that included the word 'women's,' as in 'women's chess club captain.' And it downgraded graduates of two all-women's colleges, according to people familiar with the matter."[167] In addition, the algorithm

161. Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMMUNICATIONS OF THE ACM 44 (2013), https://arxiv.org/abs/1301.6822 [https://perma.cc/T2Q7-XF2B].

162. AGRAWAL ET AL., *supra* note 5, at 195–96.

163. Anja Lambrecht & Catherine Tucker, *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads* (March 9, 2018), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852260 [https://perma.cc/KUC4-MY46].

164. *How an Algorithm May Decide Your Career*, *supra* note 62.

165. AGRAWAL ET AL., *supra* note 5, at 196.

166. Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women,* REUTERS BUSINESS NEWS (Oct. 9, 2018, 8:12 AM), https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G [https://perma.cc/QD2P-GSFG].

167. *Id.*

"favored candidates who described themselves using verbs more commonly found on male engineers' resumes, such as 'executed' and 'captured.'" [168]

Similarly, using a video game to screen applications may disadvantage older applicants because, as a group, older applicants do not perform as well on the games as younger applicants do.[169]

These potential sources of bias raise the specter of disparate impact discrimination.[170] Disparate impact discrimination occurs when a facially neutral hiring criterion, such as success in a video game "interview," has the unintended effect of disproportionately excluding members of a protected classification such as race,[171] sex,[172] or age.[173] To prevail, a person claiming disparate impact discrimination must point to a specific employment practice that causes the discriminatory impact—which, as described below,[174] may be difficult if the particular practice is buried in the "black box"[175] of an algorithm. If the person can show that the elements of the employer's decision-making process cannot be separated out for analysis, the entire decision-making process (presumably, the output of the algorithm) may be analyzed so it may become difficult for a plaintiff to isolate a specific discriminatory practice (unless courts permit plaintiffs to show the algorithm

168. *Id*.; *see also* Jerry Kaplan, *Why Your AI Might Be Racist*, WASH. POST (Dec. 17, 2018, 2:04 AM), https://www.washingtonpost.com/opinions/2018/12/17/why-your-ai-might-be-racist/ [https://perma.cc/J6U5–8VEN] (demonstrating how use Google searches display "algorithmic biases," particularly on racial grounds).

169. Catherine Rampell, *Your Next Job Application Could Involve a Video Game*, N.Y. TIMES MAGAZINE (Jan. 22, 2014), http://www.nytimes.com/2014/01/26/magazine/your-next-job-application-could-involve-a-video-game.html [https://perma.cc/XL9B-NTSA]; Taylor Casti, *Video Games Could One Day Replace Job Interviews*, THE HUFFINGTON POST (Jan. 23, 2014), http://www.huffingtonpost.com/2014/01/23/video-games-job-interviews-applications-startups_n_4647245.html [https://perma.cc/C9KK-GCXM]; Anastasia Anashkina, *Will Video Games Replace Job Interviews?*, CNN MONEY, http://money.cnn.com/video/pf/2014/01/09/pf-job-search-video-game-tests.cnnmoney/ [https://perma.cc/N3HQ-THVM]. For a more general discussion of the potential age discrimination effects of online platforms, see Ifeoma Ajunwa, *Age Discrimination by Platforms*, 40 BERKELEY J. EMP. & LAB. L. 1 (2019); *see also* Jessica K. Sink & Richard Bales, *Born in the Bandwidth: "Digital Native" As Pretext for Age Discrimination in Hiring*, 31 ABA J. LAB. & EMP. L. 521 (2016) (arguing that although digital proficiency may be a valid job criterion, using the phrase "digital native" in a job listing is an illegal age-based qualifier). However, one study found that has found that "older" players compensated for slower reaction times by more effectively planning and employing a successful strategy. Teresa Tanoos, *Brain Function Peaks at 24, But It's Not All Downhill*, EMAXHEALTH (Apr. 19, 2014, 5:01 PM), http://www.emaxhealth.com/11400/brain-function-peaks-24-its-not-all-downhill The age range in the study was ages 16–44 [https://perma.cc/6GYS-A9HD].

170. For a specific discussion of applying antidiscrimination law to online job advertising, see Pauline Kim & Sharion Scott, *Discrimination in Online Employment Recruiting*, 63 ST. LOUIS U. L.J. (forthcoming 2019). For a more general discussion of applying the disparate impact doctrine to AI and data mining, see Andrew D. Selbst & Solon Barocas, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

171. Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-2 (2012).

172. *Id*.

173. Age Discrimination in Employment Act, 29 U.S.C. §§ 623–634 (2012).

174. *See infra* Part II.A.2.

175. AGRAWAL ET AL., *supra* note 5, at 197; *see generally* Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085 (2018).

as a whole produced the impact).[176] Under established precedent, once discriminatory impact is shown by an employee, the burden of persuasion shifts to the employer, who must show the employment criterion is job-related—in other words, that the characteristics screened for on a job test or video-recorded interview or video game correlate with success on the job. The employer must also show that it is a business necessity—that the characteristics screened for are important for the business, and not merely of peripheral concern.[177]

The use of AI may make the employee's burden of proof difficult. An employee is not only at a disadvantage in identifying bias when that bias is embedded in a hiring algorithm using dozens of factors and shrouded in code, but also has scant ability to penetrate an employer's claim of job-relatedness and business necessity to contest whether the claim is justified.[178] Thus, for example, if a job candidate believes that an employer's facially neutral job screening criteria are inherently biased and thus have a discriminatory impact, it is very possible that neither the employer nor the plaintiff's attorney has any idea—and no way of finding out—what criteria the algorithm taught itself to use, where it got those criteria, and why it "chose" to use those criteria. An AI algorithm is not like a typical computer program, where an employer might tell the computer to weed out all applicants who don't have an engineering degree, didn't graduate from a top-100 school, and didn't have a GPA of at least 3.0. Instead, the employer tells the algorithm to identify the best engineers, and then the algorithm uses a vast array of data collected from disparate sources to choose its own variables, to weight those variables, and sort applicants accordingly. It may not be possible to reverse-engineer the algorithm's "thinking" process to figure out exactly how or why it did all this.

2. AI Is a Black Box

One reason that AI poses particularly troubling discrimination concerns is that each AI algorithm is a practically impenetrable black box. If an algorithm is producing biased outcomes, it is difficult if not impossible to "drill down" into the algorithm to find out what is producing the bias and how to fix it.[179] The complexity and obscurity of the algorithm poses problems for identifying and fixing bias, as well as for any litigation that results from discriminatory hiring decisions based on the algorithm. In litigation, if it is not possible to discover exactly how the algorithm is

176. Watson v. Fort Worth Bank & Trust, 487 U.S. 977 (1988).

177. 42 U.S.C. § 2000e-2(k)(1)(A)(i).

178. The problem of AI generating inscrutable decision-making is explored in Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explaining Machines*, Andrew D. 87 FORDHAM L. REV. 1085 (2018).

179. AGRAWAL ET AL., *supra* note 5, at 197.

producing bias, then a disparate impact analysis must be used to analyze the algorithm as a unitary whole for purposes of ascertaining discrimination.[180]

This is not to say that the same problems do not occur in the absence of AI. It is also difficult to identify bias when discrimination results from human beings sorting through thousands of resumes, using ad hoc or vague selection criteria.[181] Human minds often are as inaccessible as algorithmic black boxes, and absent objective or circumstantial evidence of discriminatory intent, identifying precisely how or why an HR officer's review of resumes results in discrimination can be every bit as elusive as discovering the cause of discrimination in an algorithm. Nonetheless, the inscrutability of algorithmic personnel decisions changes the way disparate impact cases are analyzed.[182]

A disparate impact challenge to the use of AI in hiring would have to begin by assessing the result and showing that the use of AI has produced a result that is disadvantageous for applicants on the basis of their race, sex, age, disability, or some other protected characteristic.[183] Plaintiffs should be required to show only that an algorithm as a whole caused a disparate impact; they should not be expected to show precisely how the algorithm produced the bias.

If a plaintiff makes this showing, then the burden should be squarely on the employer to reverse-engineer the algorithm, explain how it made its hiring recommendations, and demonstrate that each factor going into the recommendation is consistent with business necessity. An AI savvy software engineer may be needed to create a hypothesis about what might be causing the differences, provide the algorithm with different data to test the hypothesis, and compare the resulting predictions.[184]

3. AI's Potential to Reduce Bias

Though AI has the potential to create bias, it also has the potential to reduce it, in several ways. First, AI can be used to minimize the role of humans in the hiring process, and thus can eliminate or reduce the tendency of humans to hire the applicants who most resemble themselves.[185] That is,

---

180. *See supra* note 175 and accompanying text. Moreover, the problem is especially difficult at the pleading stage, before discovery, in light of Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007), and Ashcroft v. Iqbal, 556 U.S. 662 (2009) (requiring complaints in federal litigation to provide sufficient facts to make the allegations "plausible"). This may also lead to increases in removal motions by employer defendants when federal antidiscrimination statutes are raised in state court. The added expense of litigating these motions increases the burden on plaintiffs who must either consent to having their cases heard in federal court with higher pleading standards or waste resources fighting these removal motions.

181. Savage & Bales, *supra* note 44, at 223.

182. *See* Selbst & Borocas, *Intuitive Appeal*, *supra* note 175, at 1104–06.

183. *See* AGRAWAL ET AL., *supra* note 5**,** at 197.

184. *See id*. at 197–98.

185. Hoffman et al., *supra* note 53, at 4; Leigh Alexander, *Is an Algorithm Any Less Racist than a Human?*, THE GUARDIAN (Aug. 3, 2016, 2:00 PM), https://www.theguardian.com/technology/2016/aug/03/algorithm-racist-human-employers-work [https://perma.cc/K9W9–5ETE].

AI potentially can function much like a screen in a musician's orchestral audition that hides the gender of the candidates, thereby taking gender out of the process and resulting in a larger proportion of women hired.[186] AI provides a virtual screen that could reduce the number of opportunities for bias to leak into the hiring process.[187]

Similarly, AI can reduce or eliminate unconscious bias. Unconscious bias can infect the traditional hiring process both because human interviewers tend to prefer applicants most like themselves, and because humans often make unconscious assumptions about differences in abilities—such as that men perform better than women on mathematical tasks.[188] By reducing or eliminating the human role in the hiring process, the opportunities for unconscious discrimination to infect the process should be reduced commensurately.[189]

Third, AI can reduce bias by making it possible to identify and eliminate hiring practices that appear neutral but have an exclusionary impact. For example, the company Textio uses AI to improve job descriptions.[190] It found that a job description for a position that is said to involve "developing" a team draws more female applicants than one described as involving "managing" a team.[191] Similarly, AI can flag race- or sex-based differences in pay, and may even be able to find evidence of harassment or discrimination that human managers have overlooked.[192]

Any salutary effect of AI will be for naught, however, if the AI hiring algorithm is itself infected by bias, either from the programmers themselves or from the use of tainted input data, as described above. Two safeguards can reduce this possibility. First, algorithms created by multiple people with different backgrounds, perspectives, and biases can help avoid, or identify and eliminate, biases that might be present if programmers worked individually.[193] Second, it might be possible to design an algorithm that can identify and eliminate discrimination and graft it onto the algorithm used in

186. *See* Claudia Goldin & Cecilia Rouse, *Orchestrating Impartiality: The Impact of "Blind Auditions on Female Musicians*, 90 AM. ECON. REV. 715, 737–38 (2000); *see also* Pauline T. Kim, The Limits of Privacy Law as Anti-Discrimination Law in a World of Big Data (Sept. 2018) (unpublished article) (on file with author) (describing the orchestra audition study and discussing generally the interrelation of discrimination and privacy in an era of AI).

187. *Hire Education*, *supra* note 6.

188. Shana Lebowitz, *3 Unconscious Biases that Affect Whether You Get Hired*, BUSINESS INSIDER (Jul. 17, 2015, 11:47 AM), http://www.businessinsider.com/unconscious-biases-in-hiring-decisions-2015–7 [https://perma.cc/2W7S-2992].

189. Don Peck, *They're Watching You at Work*, THE ATLANTIC (Dec. 2013), http://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/ [https://perma.cc/MBR4-T4KP].

190. *Textio Hire*, TEXTIO, https://textio.com/products/ [https://perma.cc/MBR4-T4KP] (last visited Nov. 11, 2019).

191. *Hire Education*, *supra* note 6.

192. *AI-Spy*, *supra* note 6.

193. Savage & Bales, *supra* note 44, at 227; Alexander *supra* note 185.

hiring.[194] However, because discrimination can be subtle and its manifestations can change over time, any corrective algorithmic would itself require frequent audits and adjustment.

The above discussion highlights the need for EEOC regulation on algorithmic hiring. Employers using algorithms in the hiring process should be legally required to conduct regular audits[195] of the algorithm both to identify the specific data used to train the algorithm and to ensure the outcome of the algorithm is unbiased.[196] Code may need to be re-written—and an employer should not be able to avoid this obligation if the algorithm is owned and/or operated by an entity other than the employer[197] (e.g., the sex-based job ads on Facebook described above[198]).

B. Worker Privacy

As discussed above, companies using AI collect immense amounts of information about employees' work lives, habits, and dispositions that could affect their employment prospects for their entire careers. Electronic surveillance and monitoring raise potential legal issues involving employee privacy. There are several federal and state statutes as well as common law doctrines that protect some aspects of employee privacy, but these statutes (with the notable exception of the California Consumer Privacy Act, discussed below) were enacted before AI made possible the massive collection and crunching of data that are available to employers today. Thus they do not address the problem of scale and scope of today's surveillance

194. Lauren J. Young, *Computer Scientists Find Bias in Algorithms*, IEEE SPECTRUM (Aug. 21, 2015), http://spectrum.ieee.org/tech-talk/computing/software/computer-scientists-find-bias-in-algorithms [https://perma.cc/XA4R-JEAG].

195. *See* AGRAWAL ET AL., *supra* note 5, at 198.

196. Daugherty & Wilson, *supra* note 5, at 121; s*ee* Kim, *Auditing Algorithms*, *supra* note 160 at 191 (noting that "the law permits the use of auditing to detect and correct for discriminatory bias."). At least one algorithmic auditing firm already exists: *see* ORCAA, http://www.oneilrisk.com/ [https://perma.cc/V8KZ-D5UV] (website of company that audits for accuracy, bias, and fairness). Note, however, that third-party auditing of *online* algorithms may be prohibited or restricted by current law, making it difficult for academics or researchers to discover bias. *See Sandvig v. Sessions — Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online*, Am. Civil Liberties Union (Sept. 12, 2017) https://www.aclu.org/cases/sandvig-v-barr-challenge-cfaa-prohibition-uncovering-racial-discrimination-online?redirect=cases/sandvig-v-sessions-challenge-cfaa-prohibition-uncovering-racial-discrimination-online [https://perma.cc/L5UF-YXKR] (describing litigation challenging the constitutionality of the Computer Fraud and Abuse Act, which makes it a federal crime to access a computer in a manner that "exceeds authorized access").

197. See Paul Harpur, *Collective Versus Individual Rights: The Able Worker and the Promotion of Precarious Work for Persons with Disabilities Under Conflicting International Law Regimes*, 41 LOY. L.A. INT'L & COMP. L. REV. 51, 69 (2018) (discussing the challenges of gig companies altering software sourced from other companies).

198. *See supra* notes 158–160 and accompanying text (discussing how Facebook permits advertisers—including job recruiters—to target demographically restricted audiences).

capabilities. [199] Moreover, neither existing statutes nor the common law require employers to get any form of consent before using AI to monitor employees (particularly on the job) and their social media use.

The relevant federal statutes are the Electronic Communications Privacy Act (ECPA),[200] which includes the Wiretap Act and the Stored Communications Act, and the Computer Fraud and Abuse Act.[201] In addition, twelve states have statutes that outlaw the recording of conversations without the consent of all parties.[202] Moreover, two states require employers to provide notice of electronic monitoring and twenty-five states provide some protection for employee social media passwords and personal emails.[203] Title I of the EPCA, known as the Wiretap Act[204], is of limited applicability to prevent employer surveillance because it prohibits only the interception of electronic information, not access to information that has already been transmitted. Moreover, it does not apply to communications where which one party has consented. If employers own the email or communications system used by employees, the employees may be deemed to have given consent.[205] The Wiretap Act also does not apply to other forms of monitoring, such as GPS and electronic wearable devices.

Title II of the EPCA, the Stored Communications Act (SCA), is also limited in its ability to protect worker privacy.[206] The SCA protects individuals' private communications held in electronic storage by third parties.[207] Though the SCA does not explicitly mention social media accounts, such accounts have been found to fall within the statute's definition of electronic storage.[208] However, social media content that is publicly available is not likely to not be protected by the SCA, because such content is not considered "private."[209] On the other hand, content shared privately—sent directly to only a select group of people, or posted using privacy settings that restrict public access—might be protected, such that an employer's monitoring it would violate the statute.[210]

---

199. See William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 EMP. RTS. & EMP. POL'Y J. 49 (2008); See Robert Sprague, *Survey of (Mostly Outdated) Laws Affecting Workplace Monitoring*, 93 CHI-KENT L. REV. 221 (2018).

200. 18 U.S.C. §§ 2510–2511 (2012).

201. 18 U.S.C § 1030 (2012).

202. Sprague, *supra* note 199, at 242–43.

203. *Id*. at 243.

204. 18 U.S.C. § 2511 (2012).

205. Ifoema Ajunwa, Kate Crawford, & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 736, 749 (2017) [hereinafter *Limitless Surveillance*].

206. 18 U.S.C. § 2701(a) (2012).

207. *Id*.

208. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

209. European law may provide workers with more protection than American law. *See* IBA, *supra* note 7, at 110–13.

210. *Crispin*, 717 F.Supp.2d at 991; Pietrylo v. Hillstone Restaurant Group, No. 06–5754-FSH, 2008 WL 6085437, at *1–2 (D.N.J. July 25, 2008); *see also* Christopher J. Borchert, Fernando M. Pinguelo &

However, there is considerable authority weighing against applying the SCA to social media accounts.[211] First, there are conflicting views about what constitutes "electronic storage" for purposes of the statute. Some courts have held that once an email or electronic communication is read, it is no longer in storage and hence not within the statute.[212] Moreover, courts disagree about the application of the statute's exceptions. For example, in *Fraser v. Nationwide*, the Third Circuit held that an employer's search of an employee's email was not a violation of the SCA because the SCA excepts seizures of email authorized "by the person or entity providing a wire or electronic communications service."[213] In *Fraser*, the employer was the entity providing the electronic communications service through its email servers, so there was no violation.[214]

Employee surveillance has also been challenged as violating the Computer Fraud and Abuse Act (CFAA).[215] That statute creates civil and criminal violations for an individual who intentionally accesses a computer without authorization.[216] However, the statute has been interpreted to permit employers to access employee electronic information when the data is stored on the employer's own computer or network.[217]

Overall, existing federal laws are weak vehicles for protecting employee privacy in the face of the multitude of employer surveillance and monitoring tools currently in use.[218] Moreover, state laws offer little additional protection. The one possible exception is California Consumer Privacy Act (CCPA), which was enacted in 2018 and will become effective on January 1, 2020.[219] The CCPA is the first omnibus privacy regulation in the United States and is modeled after the European General Data Protection Regulation (GDPR).[220] The CCPA, among other things, gives a "consumer a right to request a business to disclose the categories and specific pieces of personal

---

David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36 (2015); Patricia Sánchez Abril, Avner Levin & Alissa Del Riego, *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63, 83, 87 (2012).

211. *See generally Limitless Surveillance*, *supra* note 205, at 749–50.

212. *See* Sprague, *supra* note 199, at 23, n. 78.

213. 352 F.3d 107, 114–15 (3d. Cir. 2003) (citing 18 U.S.C. § 2701(c)(1) (2012))..

214. *Id*.

215. *See, e.g.*, Owens v. Cigna, 188 F. Supp 3d 790, 793 (N.D. Ill. 2016).

216. 18 U.S.C §§ 1030(12)(g), 12(h).

217. *See Owens*, 188 F. Supp. 3d at 793.

218. *Limitless Surveillance*, *supra* note 205, at 748–50.

219. Assem. B. 375, 2017–18 Reg. Sess. (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 [https://perma.cc/R6ZY-9LDK].

220. *See* Andrei Gribakov, *Road to Adequacy: Can California Apply Under the GDPR?*, LAWFARE (Apr. 22, 2018, 8:30 AM), https://www.lawfareblog.com/road-adequacy-can-california-apply-under-gdpr [https://perma.cc/7Y5E-8YKB]; *US State Omnibus Privacy Law-A Primer*, BAKER MCKENZIE (Jul. 3, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/07/us-state-omnibus-privacy-laws [https://perma.cc/9BZN-GVT9].

information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared."[221] It also gives consumers the right to request that companies delete their personal information, and requires companies receiving such a request to do so.[222] Rulemaking by the California Attorney General's Office is ongoing as this article is being prepared for publication,[223] and it is not yet clear whether or to what extent the CCPA might protect workers from surveillance and monitoring.

In addition to the privacy concern with surveillance and monitoring, electronic data collection and AI databases have the potential to create a permanent electronic resume for individual workers that can be neither erased nor challenged. Whether that occurs depends upon the several legal issues that are not yet resolved. First, do workers have an ownership interest in data compiled about them? And if so, under what circumstances can they exclude others from seeing or using it? If not, do they have a right to access the data? Second, do they have any protection from this data being shared with others—such as to prospective employers—or does their data travel with them as a lifetime electronic resume that they can neither see nor rebut? And third, do workers have recourse if their data is incorrect and it is used in an adverse employment action or is shared with others?

One example illustrates the potential problems. As described above, HireVue makes and analyzes pre-hire videos to determine evaluate job candidates.[224] Under current U.S. law, HireVue owns the videos—just as Facebook argues that it owns, or at least has the right to use, the user-generated data supplied by its users, and just as Google owns the data it has gathered from online searches on its platform.[225] If an applicant interviews for a job through HireVue, can she demand that HireVue delete her video-recorded interview after the job search is over? The answer would probably be yes under European data privacy laws,[226] but there is no equivalent data

221. *Id*.

222. *Id*.

223. *See CCPA Current Rule Making Activity*, STATE OF CAL. DEP'T OF JUST. OFF. OF THE ATT'Y GEN, https://oag.ca.gov/privacy/ccpa [https://perma.cc/M9TD-77TM] (last visited Sept. 29, 2019).

224. *See supra* Part I.B.1.b(ii) (Video-recorded Interviews).

225. *See* David Lazarus, *Facebook says you 'own' all the data you post. Not even close, say privacy experts*, L.A. TIMES (Mar. 18, 2018), https://www.latimes.com/business/lazarus/la-fi-lazarus-facebook-cambridge-analytica-privacy-20180320-story.html [https://perma.cc/X3V5-WP22] ("Regardless of what a company's privacy policy may say, it's a certainty that people's information will be bought and sold for commercial or political purposes")

226. The EU General Data Protection Regulation (GDPR) Article 17 provides a "right to be forgotten" (also known as "data erasure"). Council Regulation 2016/679, art. 17, 2016 O.J. (L 119). It entitles a person to require an entity holding data on the person to erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. *Id.* The conditions for erasure include the data no longer being relevant to original purposes for processing (in this context, the original job interview), or the person withdrawing consent. *See id*.

privacy law in the U.S. Instead, HireVue's Privacy Policies explain that it collects, retains, and stores information on individual applicants that the individuals provide voluntarily or that it collects from third party sources or potential employers.[227] It also collects data from an applicant's own devices or from cookies or other technological tracking devices. HireVue further states that individuals have a right to request that data be deleted, but it does not guarantee that any such request will be honored.[228] Thus, under its policies, if an individual interviews through HireVue for a second job, HireVue can access the video from her first application to refine its analysis of her. Indeed, it can potentially create an "applicant profile" of her that will follow her throughout her life.[229] It is as yet unknown the extent to which companies consolidate, pool, and share employee information culled from electronic collective sources, but if they do, then one bad interview day could mar an applicant's job prospects for life.

C. AI and the Antitrust Laws

If competing companies share information about employees and use that information to make hiring, discipline, promotion or other decisions, they run into several potential antitrust issues. The Sherman Antitrust Act prohibits concerted activity that results in an unreasonable restraint of trade.[230] It applies not only to overt price fixing and conspiracies to harm competitors, but also to activities that affect employees. For example, in *Freeman v. Eastman-Whipstock Inc*., the District Court for the Southern District of Texas stated that an employee who alleged he had been blackballed had standing under the antitrust law.[231] Similarly, in *Quinonez v. National Association of Security Dealers*, the Fifth Circuit ruled that a former employee stated a claim under the Sherman Act when he alleged he was denied employment "not because of any individual consideration of his own merits or qualifications," but because the firms had agreed among themselves "that they would not 'pirate' the others and would deny employment to applicants who had either

227. *See Hirevue Privacy Notice*, HIREVUE (May 17, 2018), https://www.hirevue.com/company/privacy [https://perma.cc/C59X-ZJ7T].

228. *See id.*

229. *See id.*

230. "Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations, is hereby declared to be illegal." 15 U.S.C. §1 (2012).

231. 471 F.2d 685, 689 (S.D. Tex. 1975). The court stated that "a plaintiff [has] standing under the antitrust laws to allege and challenge a conspiracy of two or more employers attempting to prevent one's employment in an industry, where those conspirators have the power to enforce their conspiratorial decision. *Id.* at 689–90, citing *Radovich v. NFL*, 352 U.S. 445, 453 (1957); *see also* F.S. Tinio, Annotation, *Validity Under the Federal Antitrust Laws (15 U.S.C.A. §§ 1 et seq.) of Agreements Between Employers or Employer Associations Imposing Restrictions on Employment*, 2 A.L.R. Fed. 839 (1969).

been fired or who had been rejected for employment by any other member firm."[232]

Because AI facilitates information gathering, storage, retention, and sharing, its use in personnel matters can implicate the antitrust laws. For example, if several competitors shared AI-gleaned information regarding employee performance, personal characteristics, social media history, medical absenteeism, and other such data, this might run afoul of the antitrust laws if done with the intent of using the information to blackball workers deemed undesirable, or to determine whom to hire and how much to pay them. Similarly, consider an HR services company that uses AI to conduct video job interviews of prospective employees, uses data analytics to construct a personality profile and predict future performance from those interviews, then sells that information to all companies who pay for its services. This too could be an unlawful restraint of trade. These and other similar scenarios are explored below.

1. Application of the Antitrust Laws to Collaboration Between Employers

As discussed above, the antitrust laws apply to restraints on competition by employers for their personnel practices.[233] If employers use shared employee information amassed through AI and electronic surveillance to set compensation, engage in a no-raiding agreement, or blacklist an employee, they could face significant antitrust implications.[234]

In this section, we will discuss the antitrust issues posed by using AI in personnel management to facilitate collaborations among competitors in general, including issues arising from exchanges of salary and benefit information or other AI-gleaned employee information. In the next section, we consider boycotts of particular employees and the legality of no-poaching agreements in the AI setting.

2. Collaboration Among Competitors

The U.S. Federal Trade Commission's ANTITRUST GUIDELINES FOR COLLABORATION AMONG COMPETITORS state that a competitor collaboration "comprises a set of one or more agreements, other than merger agreements, between or among competitors to engage in economic activity, and the economic activity resulting therefrom."[235] Competitors are permitted to collaborate on matters of research and development, production,

232. 540 F.2d 824, 827 (5th Cir. 1976).

233. Mark W. Pletcher & Ludovic C. Ghesquiere, *In Restraint of Trade: The Judicial Law Clerk Hiring Plan*, 78 U. COLO. L. REV. 147, 168 (2007).

234. *See* Daniel I. Booker, *Antitrust and Employment*, ANTITRUST, Fall 1996, at 33.

235. U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR COLLABORATIONS AMONG COMPETITORS (2000) at 2, http://www.ftc.gov/os/2000/04/ftcdojguidelines.pdf, [https://perma.cc/DP2B-RDLM] [hereinafter Competitor Collaboration Guidelines].

marketing, distribution, sales or purchasing, as well as information sharing, so long as they are not using the collaboration to impede competition.[236]

In determining whether a collaboration violates antitrust law, there are two basic tests.[237] First, if an agreement tends to raise prices or reduce output, the agreement is illegal per se.[238] In addition to an explicit agreement, an illegal-per-se agreement can "be established through circumstantial evidence of 'business behavior which evidences a unity of purpose or a common design and understanding, or a meeting of the minds in an unlawful arrangement.'"[239] If there is no agreement or business behavior evidencing a common purpose or explicit agreement concerning conduct that is illegal per se, a second test, known as the rule of reason, is applied.[240] The "rule of reason" test is applied to determine the overall competitive effect of an agreement or course of conduct that does not fall within the prohibitions of the "illegal per se" rule.[241] The enforcement agency will look at the nature of the agreement, its business purpose, the anti-competitive harm, and any pro-competitive benefits. It looks at factors such as the market share of the participants, whether the agreement is exclusive or non-exclusive, its duration, and whether the agreement facilitates collusion.[242]

In the area of labor relations, employers violate antitrust law when they make an explicit or implicit agreement with other employers to fix wages or to determine whom to hire. Indeed, the Department of Justice treats blatant compensation fixing as a criminal violation.[243] Additionally, if there is found to be such an agreement, the employee or other injured party can sue for triple damages.[244] Thus, for example, it would be a violation if an employer makes

---

236. JULIAN O. VON KALINOWSKI, ANTITRUST LAWS AND TRADE REGULATION § 16.01 (2d ed. 2019).

237. There is also a third test, the "quick look" test that falls in between per se and rule of reason. "[T]he 'quick look' analysis is an abbreviated form of the rule of reason that may be used when 'an observer with even a rudimentary understanding of economics could conclude that the arrangements in question could have an anticompetitive effect on customers and markets.'" United States v. eBay, Inc., 968 F. Supp. 2d 1030, 1037 (N.D. Cal. 2013).

238. Competitor Collaboration Guidelines, *supra* note 235, at 3.

239. Cason-Merenda v. Detroit Med. Ctr., 862 F. Supp. 2d 603, 625 (E.D. Mich. 2012) (quoting Wallace v. Bank of Bartlett, 55 F.3d 1166, 1168 (6th Cir. 1995)).

240. In re Baby Food Antitrust Litig., 166 F.3d 112, 117–18 (3d. Cir. 1999) (citing United States v. U.S. Gypsum Co., 438 U.S. 422, 441 n. 16 (1978)).

241. *Id*. *See, e.g.*, Continental Television v. GTE Sylvania, 433 U.S. 36 (1977) (nonprice vertical restraints on the number of franchisees); State Oil v. Khan, 522 U.S. 3 (1997) (maximum resale price maintenance agreements); Leegin Creative Leather Products, Inc. v. PSKS, Inc., 551 U.S. 877 (2007) (minimum resale price maintenance agreements).

242. KALINOWKSI, *supra* note 236, § 16.03.

243. Michael Lindsay, Jaime Stilson & Rebecca Bernhard, *Employers Beware: The DOJ and FTC Confirm That Naked Wage-Fixing and "No-Poaching" Agreements Are Per Se Antitrust Violations*, ANTITRUST SOURCE, December 2016 at 1 (citing U.S. DEP'T OF JUSTICE ANTITRUST DIV. & FED. TRADE COMM'N, ANTITRUST GUIDANCE FOR HUMAN RESOURCE PROFESSIONALS 2 (2016), https://www.justice.gov/atr/file/903511/download [https://perma.cc/3EEW-499Z] [hereinafter HR GUIDANCE]).

244. HR GUIDANCE, *supra* note 243, at 2–3.

an agreement with another company about employee salary or other terms of compensation, either at a specific level or within a range (so-called wage-fixing agreements). [245] Similarly, explicit no-poaching agreements between employers is a violation.[246]

A joint bulletin by the Federal Trade Commission and the Department of Justice's Antitrust Division gives several examples of conduct it considers unlawful. In the last few years, the Department of Justice sued three technology firms for engaging in no-poaching agreements.[247] And, in 2007, it sued the Arizona Hospital Association because the member hospitals agreed to set a schedule of pay rates for per diem nurses.[248] The Bulletin concludes that "[g]oing forward, the DOJ intends to proceed criminally against naked wage-fixing or no-poaching agreements. These types of agreements eliminate competition in the same irredeemable way as agreements to fix product prices or allocate customers, which have traditionally been criminally investigated and prosecuted as hardcore cartel conduct."[249] The potential for an administrative action in this area would seem to be buttressed by hearings held in 2018 by the FTC on the antitrust implications of pricing algorithms.[250]

a. Sharing Salary Information

AI provides a myriad of opportunities for companies to share salary information in potential violation of antitrust laws. For example, an HR service provider using AI to recommend salaries could aggregate data from several companies in the same industry. Similarly, industry-specific employer associations could use AI to mine and share data on either individual employees or for particular job descriptions in the aggregate. The question is whether antitrust laws—which were not designed with employment, much less the use of AI in employment, in mind—can be used to regulate or prohibit this kind of conduct.

A per se unlawful agreement to fix salaries not only includes an explicit oral or written agreement, but can "be established through circumstantial evidence of 'business behavior which evidences a unity of purpose or a common design and understanding, or a meeting of the minds in an unlawful arrangement.'"[251] Evidence of discussions and parallel behavior may result

245. *Id*.

246. *Id*.

247. *Id*. at 3–4.

248. *Id*. at 3.

249. *Id*. at 4.

250. *See* LATHAM & WATKINS, *DEEP DIVE ON DEEP LEARNING: FTC CONSIDERS ARTIFICIAL INTELLIGENCE* 1, (2018), https://www.lw.com/thoughtLeadership/lw-deep-dive-deep-learning-ftc-considers-artifical-intelligence [https://perma.cc/NC74–35XM] [hereinafter *Deep Dive*].

251. *See* Cason-Merenda v. Detroit Med. Ctr., 862 F. Supp. 2d 603, 625 (E.D. Mich. 2012) ((quoting Wallace, 55 F.3d at 1168) (quotations marks and citations omitted).

in a per se violation, because one can infer the parties implicitly agreed to fix wages.[252] Funneling the information through a third party can constitute a per se violation, for which there are criminal and civil penalties.[253] Thus, for example, in 2018, the FTC brought (and settled) a case against two staffing agencies who had agreed to reduce the rate they paid to the physical, speech, and occupational therapists that the agencies supplied to home health agencies on a contract basis.[254]

Even if there is no per se agreement to fix salaries, exchanging salary information can have anti-competitive effects under the rule of reason test. Courts look to a variety of factors under this test such as whether the information is: "(1) current and future information; (2) company-specific; (3) not publicly available; (4) exchanged regularly; and (5) shared with the knowledge that it would be used to make compensation decisions."[255] As the Department of Justice joint bulletin explains:

> [w]hile agreements to share information are not per se illegal and therefore not prosecuted criminally, they may be subject to civil antitrust liability when they have, or are likely to have, an anticompetitive effect. Even without an express or implicit agreement on terms of compensation among firms, evidence of periodic exchange of current wage information in an industry with few employers could establish an antitrust violation because, for example, the data exchange has decreased or is likely to decrease compensation.[256]

For example, one court has held that an annual salary survey of medical residents could be an unreasonable restraint of trade when used in conjunction with a matching program for job placements.[257] This was true even if the association issuing the survey did not discuss compensation for residents with the medical schools, because it was reasonable to infer the association shared the information with member medical schools to facilitate price-fixing of salaries.[258] The fact that the survey was publicly disseminated did not negate an antitrust violation because medical residents received only one offer and could not use the information to bargain with another hospital.[259]

---

252. HR GUIDANCE, *supra* note 243 at 3.

253. *See id.* at 3–4.

254. *See* Mary Strimel, *THE LATEST: FTC Settles Civil Complaint for Wage-Fixing*, ANTITRUST ALERT (Aug. 2, 2018), https://www.antitrustalert.com/2018/08/articles/ftc-developments/the-latest-ftc-settles-civil-complaint-for-wage-fixing/ [https://perma.cc/2NKE-6665].

255. Toby G. Singer, *Antitrust Implications of Surveys and Other Forms of Information Sharing*, *in* LEGAL ISSUES AFFECTING ACADEMIC MEDICAL CENTERS AND OTHER TEACHING INSTITUTIONS, AM. HEALTH L. ASSOC. SEMINAR MATERIALS, AHLA-PAPERS P01270503, 1–2 (Jan. 17, 2005).

256. HR GUIDANCE, *supra* note 243, at 4–5.

257. *See* Jung v. Ass'n of Am. Med. Colls., 300 F. Supp. 2d 119, 165–66, 173–74 (D.D.C. 2004). Note that this decision occurred before legislation specifically exempting medical resident matching programs from antitrust laws. *See* Singer, *supra* note 255, at 4.

258. *See Jung*, 300 F. Supp. at 166–67.

259. *Id.* at 167–68.

In *Todd v. Exxon Corp.*,[260] the Second Circuit applied the rule of reason test to determine that the Plaintiffs had plead sufficient allegations that an agreement among six major oil companies to share salary information could mount to an illegal salary-fixing agreement. The relevant factors were "the specificity of the information exchanged, the defendants' alleged market dominance, the concentrated nature of the industry, the employees' inability to simply switch to other types of employers, and the defendants' express agreement to use the information in setting salaries."[261] While the information was channeled through a third-party aggregator, the data was reported in such a way that it was easy to discern the information needed to coordinate employee salaries.[262] Moreover, the Plaintiffs alleged that companies conducted regular meetings to discuss salaries.[263]

There have also been several lawsuits alleging collusion by hospitals on nurses' salaries.[264] One case involved regular aggregate surveys as well as frequent exchanges of non-aggregated compensation information among hospitals' HR personnel, either through phone calls or at industry meetings.[265] The "aggregate" survey data was distributed in disaggregated form so that it was easy to "crack the code" and tell which hospitals paid what compensation. Data more current than the three-month old federal guideline was included, and in some cases, so were future projected pay increases. Information sometimes went through another hospital before it went to the third-party aggregator. A federal district court found that, although there was no explicit agreement between the hospitals to suppress nurse compensation, the hospitals fell outside the "safety zone" criteria set forth in the DOJ/FTC Guidelines, and that an antitrust violation may have occurred under the rule of reason analysis.[266]

---

260. 275 F.3d 191, 214 (2d Cir. 2001).

261. WILLIAM HOLMES & MELISSA MANGIARACINA, ANTITRUST LAW HANDBOOK § 2:11 n.13 (2018).

262. Corby C. Anderson & Ted P. Pearce, *The Antitrust Risks of Information Sharing*, 23 FRANCHISE L.J. 17, 20 (2003) (discussing *Todd*, 275 F.3d 191).

263. Id.

264. See Jeff Miles, *The Nursing Shortage, Wage-Information Sharing Among Competing Hospitals, and the Antitrust Laws: The Nurse Wages Antitrust Litigation*, 7 HOUS. J. HEALTH L. & POL'Y 305, 306 (2007); *see* Lindsay et al., *supra* note 243, at 5–6.

265. *See* Cason-Merenda v. Detroit Med. Ctr., 862 F. Supp. 2d 603, 615–17 (E.D. Mich. 2012) (quoting Wallace, 55 F.3d at 1168)).

266. *Id.* at 625, 647–49. According to guidance issued for the health care industry, the government will not challenge the sharing of salary information if (1) the information is managed by a third party; (2) the data is more than 3 months old; and (3) "there are at least five providers reporting data upon which each disseminated statistic is based, no individual provider's data represents more than 25 percent on a weighted basis of that statistic, and any information disseminated is sufficiently aggregated such that it would not allow recipients to identify the prices charged or compensation paid by any particular provider." Salary-information exchanges about future compensation is likely considered anticompetitive. Additionally, enforcement agencies will consider the pro-competitive effect of exchanging salary information — it arguably promotes efficiency by ensuring producers are not paying too much for salaries. *See* Singer, *supra* note 255, at 3, (citing U.S. DEP' OF JUSTICE & THE FED. TRADE COMM'N, STATEMENTS OF ANTITRUST ENFORCEMENT POLICY IN HEALTH CARE (August 1996),

It seems highly likely that AI will be used to share salary information. If done though a data consolidator, it may not be illegal per se, and likely will be analyzed under the rule-of-reason test. It is unclear at this point how the factors described above will be applied in AI cases.

b. Sharing Other Personnel Information

Beyond exchanging salary information, an employer can violate the antitrust laws by sharing other types of information that AI-linked surveillance is designed to collect. This follows from the fact that not only is the exchange of *price* information a possible antitrust violation, but so too is exchange of *cost* information.[267] Information gleaned from electronic surveillance and AI algorithms has presumptive value to a firm's bottom line by affecting decisions regarding costs and profitability. Thus, an explicit or implicit agreement, or a practice of sharing such information, could run afoul of the antitrust prohibition on information sharing.

One area that could run afoul of the antitrust laws is sharing information about employee benefits—health care benefits, retirement contributions, the number of vacation days, and the like. As with salary information exchanges, if employers (directly or through an HR-services provider) use AI to gather data to set benefits, they could be exposed to antitrust liability.[268] Sharing information about individual job performance, employee health issues, and disciplinary infractions could also be violations if they are intentionally used to affect hiring decisions and reduce costs.

The advent of AI makes employer information-sharing more likely to occur, and more precise when it does.[269] If a company knows what its competitors are paying, it can set its employees' salaries and benefits commensurately and avoid a bidding war for talent. AI may also make it possible for one employer to mine this type of data from various sources on the web. Or, it can hire an H.R. services provider—like those described earlier in the article—to track its employees' individual productivity and recommend salary increases, bonuses, etc. That H.R. services provider may also be providing similar services to some of its competitors, and may aggregate data from each of the companies to increase the predictive power of its algorithms. In the process, it would necessarily pool, and share, salary and benefit information.

---

https://www.ftc.gov/sites/default/files/attachments/competition-policy-guidance/statements_of_antitrust_enforcement_policy_in_health_care_august_1996.pdf [https://perma.cc/2PAE-JY5H] [hereinafter DOJ/FTC Guidelines]).

267. *See* Singer, *supra* note 255, at 2–3.

268. *Id.* at 2.

269. For a low-tech version of such information sharing, *see* Rachel Nuwer, *Silicon Valley's Exclusive Salary Database*, WIRED (July 1, 2018), https://www.wired.com/story/silicon-valleys-exclusive-salary-database/ [https://perma.cc/7RXU-EWNE] (describing Option Impact, a database of tech-industry salaries compiled by and for Silicon Valley start-ups).

Courts have also found employers to be in violation of the antitrust laws when they exchange what courts term "competitively sensitive information." While the term is vague, it has been applied to information that the Department of Justice or FTC believes can be used to facilitate collusion or impede other competitors. In the AI context, such information might include salary and benefits information, applicant histories, and employee work performance, and the like.[270] On the other hand, information exchanges can also be procompetitive, as when they enable companies to learn new and more efficient methods of doing business. Thus, information exchanges between competitors are not necessarily illegal. Factors weighing in favor of a lawful information exchange include "specific plans to maintain confidentiality, use of third parties to handle the information exchange, and procompetitive effects of the information exchange. The size of the group or association involved in the exchange and the amount and type of information exchanged are also relevant."[271] It can also make a difference whether there are circumstances justifying the need for an information exchange.[272] For example, in *Cement Manufacturers Protective Ass'n v. United States*, the Court found that sharing price information was permissible because it was exchanged to protect the sellers from fraudulent buyers.[273]

On the other hand, in *United States v. Container Corp. of America,* the Court distinguished *Cement Manufacturers* because there were no such "controlling circumstance[s]."[274] In the *Container Corp.* case, the Court stated that an exchange of information about prices can be an antitrust violation even if companies have not agreed to set a particular price, especially if the exchange is of recent prices, the goods are fungible (so that price is the only distinguishing factor), and the industry is an oligarchy.[275]

Additionally, the enforcement agency considers whether an information-exchange agreement limits independent decision making by the companies involved.[276] For example, in *Black v. J.P. Morgan*, a federal district court held that lenders exchanging consumer credit information via third party credit bureaus did not violate antitrust laws because the businesses retained the responsibility of deciding for themselves whether or not to give

270. *See, e.g.* CARRIE MAHAN & NATALIE HAYES, WEIL, GOTSHAL, & MANGES LLP, NEW FTC GUIDANCE ON INFORMATION EXCHANGE HIGHLIGHTS NEED FOR SAFEGUARDS DURING DUE DILIGENCE AND INTEGRATION PLANNING 1–2 (April 16, 2018), https://www.weil.com/~/media/publications/antitrust/2018/new-ftc-guidance-on-information-exchange-highlights.pdf [https://perma.cc/5RZK-5PSZ].

271. *Information Exchanges,* [26 No. 1] CORP. COUNS. Q., Art. 2, 14 (Jan. 2010). For a chart showing risk factors for antitrust violations in information exchanges, *see* Brian R. Henry, *Benchmarking and Antitrust*, 62 ANTITRUST L.J. 483, 510 (1994).

272. *See generally Information Exchanges*, *supra* note 271 (describing examples when information exchanges are justified).

273. *See* 268 U.S. 588, 588 (1925).

274. 393 U.S. 333, 335 (1969).

275. *See id.* at 336–37.

276. Courts consider this using a rule-of-reason analysis. *See* KALINOWKSI, *supra* note 236.

credit to a particular customer.[277] As the court explained, "given the legitimate function of such data, it is not a violation of § 1 [of the Sherman Act] to exchange such information, provided that any action taken in reliance upon it is the result of each firm's independent judgment, and not of agreement."[278]

In sum, the use of shared and consolidated AI information by employers to guide personnel decisions has antitrust ramifications. The Department of Justice bulletins and the decided cases make it clear that companies can violate the antitrust laws by sharing information about employees.[279] On the other hand, if companies share information about employees for legitimate business purposes and do it through a third party employment agency or HR services provider, but do not agree on how the information should be used or how hiring decisions should be made, it is likely not an antitrust violation. To date, no cases have posed these issues, but they are likely to arise before long.

c. No Poaching Agreements

Employers can face antitrust liability if they make explicit or tacit agreements with other companies not to hire each other's employees.[280] The use of AI makes these 'no-poaching agreements' easier to implement, and harder to detect. As explained above, AI makes it possible for employers to monitor, analyze, and quantify the productivity of their workers in ways not possible before, and the proliferation of AI based HR-service providers serving multiple companies, often in the same industry, provides an easy and surreptitious mechanism for sharing such information.

For example, AI is used to ascertain which employees are the most productive or excel at certain tasks. It would violate the law if several employers share that data and agree they will not hire each other's top performers. As in the salary cases discussed above, discussions and parallel behavior by the employers can prove that such an agreement exists, even if there is no evidence of an explicit oral or written agreement.[281] In some pre-AI cases, courts apply a per se rule, and if that fails, the rule of reason analysis.[282] And also, as in the salary cases discussed above, naked poaching agreements can result in criminal as well as civil sanctions.[283]

---

277. Black v. JP Morgan Chase & Co., No. 10–848, 2011 WL 4102802, at *23 (W.D. Pa. Aug. 10, 2011).

278. *Id*. at *21 (quoting Michelman v. Clark-Schwebel Fiber Glass Corp., 534 F.2d 1036, 1048 (2d Cir. 1976)).

279. HR GUIDANCE, *supra* note 243, at 4–6.

280. *Black*, 2011 WL 4102802, at *5.

281. *See id*.

282. Lindsay et al., *supra* note 243, at 11; *In re High-Tech Emp. Antitrust Litig.*, 856 F. Supp. 2d 1103, 1114–15 (N.D. Cal. 2012).

283. HR GUIDANCE, *supra* note 243, at 4.

In general, courts find a violation of § 1 of the Sherman Act "[i]f a no-poaching agreement (1) serves no legitimate business purpose, or (2) serves a legitimate business purpose but is *not* narrowly tailored to meet that purpose."[284] If the agreement is necessary for a joint venture, merger, or some other legitimate collaboration, then it serves a legitimate business purpose.[285] So too it is lawful if it is narrowly tailored in a merger situation, if it is for a limited duration, and if it is limited to "specific key employees or identifiable categories of employees."[286]

A series of recent Silicon Valley no-poaching cases involving eBay, Intuit, Apple, Lucasfilm and several other companies illustrate the application of antitrust principles to no-poaching agreements.[287] They involved explicit bilateral agreements between direct competitors promising not to cold call each other's employees.[288] Moreover, eBay agreed not to hire anyone from Intuit for a year, and Lucasfilm promised to give notice if it made an offer to a competitor's employee and would not offer anything above its initial offer.[289] The Department of Justice found these agreements per se unlawful and the defendants eventually settled.[290]

A separate lawsuit filed by the affected employees claimed that these nearly identical bilateral agreements were interconnected.[291] The plaintiffs asserted that each agreement involved a company under the control of the late Steve Jobs or a company whose board shared at least one member of Apple's board, that senior executives from each of the tech companies negotiated and enforced the bilateral agreements, and that these executives concealed the agreements from employees and the public.[292] Additionally, the complaint stated that Steve Jobs himself attempted to negotiate a similar

284. Rochella T. Davis, *Talent Can't Be Allocated: A Labor Economics Justification for No-Poaching Agreement Criminality in Antitrust Regulation*, 12 BROOK. J. CORP. FIN. & COM. L. 279, 295 (2018).

285. Lindsay et al., *supra* note 243, at 2; *see United States v. eBay, Inc.*, 968 F. Supp. 2d 1030, 1039–40 (N.D. Cal. 2013).

286. Lindsay et al., *supra* note 243, at 10.

287. The Silicon Valley cases consist of Department of Justice enforcement actions against technology companies. *See* Complaint, United States v. Adobe Sys., Inc., No. 10-cv-01629, 2010 WL 11417874 (D.D.C. Sept. 24, 2010); Complaint, United States v. Lucasfilm Ltd., No. 10-cv-02220, 2010 WL 5344347 (D.D.C. Dec. 21, 2010); Complaint, United States v. eBay, Inc., No. 12-cv-5869, 2012 WL 5727488 (N.D. Cal. Nov. 16, 2012); *see also* United States v. eBay, Inc., 968 F. Supp. 2d 1030 (N.D. Cal. 2013) (denying eBay's motion to dismiss the complaint). These cases were settled with consent judgments. *See* Lindsay, *supra* note 243, at 7. Additionally, tech company employees filed a civil suit against their employers. *In re High-Tech Emp. Antitrust Litig.*, 856 F. Supp. 2d at 1109 (N.D. Cal. 2012). For a similar situation in the animation and visual effects business, see *Nitsch v. Dreamworks Animation SKG Inc.*, 315 F.R.D. 270, 274 (N.D. Cal. 2016).

288. Lindsay et al., *supra* note 243, at 6–7.

289. *Id.* at 6.

290. *In re High-Tech Emp. Antitrust Litig.*, 856 F. Supp. 2d 1103, 1109 (N.D. Cal. 2012).

291. *Id.* at 1108.

292. *Id.* at 1110.

agreement with the CEO of Palm.[293] The court found the employee-plaintiffs sufficiently stated a claim under the Sherman Antitrust Act.[294]

AI makes it more likely than ever that companies will enter into explicit or implicit no-poaching agreements. If an HR services provider collects, through its clients, a large volume of information about the performance of individual employees, uses that information to predict future performance, and then provides these predictions to other employers in the same industry, it could be a violation, even absent explicit concerted action.[295] This would be true if the companies involved then avoided hiring each other's top performers, or if they used the information to refuse to hire employees deemed to be "trouble-makers," as will be discussed below.

d. Boycotts and Blacklists

The previous section described how an agreement not to poach top employees can violate antitrust laws. A more frequent scenario is a modern day blacklist of employees considered 'trouble-makers.' This would occur if two or more firms agreed not to hire individuals identified through AI as undesirable. It would also occur if firms providing AI-aided HR services (such as researching and interviewing prospective employees and tracking existing employees) provide detailed information to their clients about prospective new hires, and their clients collectively decide not to hire certain individuals whom the data show to be unproductive, disruptive, oppositional, or possess other negative proclivities. As will be explained, the use of shared information to blacklist an individual can constitute an unlawful conspiracy by two or more employers to restrain that individual's participation in the labor market. On the other hand, there can be legitimate purposes for information sharing that would prevent antitrust liability, such as when the shared information is for purposes of job references or to warn of unethical or illegal conduct. The legal question with employee blacklisting is, at what point does either such active or passive collusion become illegal under antitrust law? The use of AI makes information sharing more likely to occur, more difficult to detect, and the purposes impossible to evaluate. Thus, the legal test, and the lines that are drawn, become blurry.

A blacklist of employees is essentially a group boycott of an employee by employers.[296] As with any Sherman Act violation, a blacklist could violate antitrust law if it is a concerted activity and an unreasonable restraint of

293. *Id.* at 1116–17.

294. *Id.* at 1123.

295. *Cf. id.* at 1117 (explaining that plaintiffs may state a claim under the Sherman Antitrust Act when they plead facts that "tend to exclude the possibility of independent action" (alteration and citation omitted)).

296. Booker, *supra* note 234, at 35–36; Marc Edelman, *Are Commissioner Suspensions Really Any Different from Illegal Group Boycotts? Analyzing Whether the NFL Personal Conduct Policy Illegally Restrains Trade*, 58 CATH. U.L. REV. 631, 639–40 (2009).

trade.[297] If these two criteria exist, then the per se, rule of reason or quick look test is applied to determine whether a violation occurred.[298] One antitrust expert provides a useful description of when boycotts violate the law:

> On the one hand, joint efforts to drive troublesome competitors out of business are almost surely illegal, while, on the other, it is less likely to be illegal to "boycott" a member of a business or profession who has violated reasonable ethical or industry standards. In the uncertain middle are situations involving joint action by industry groups that may seem political but have a commercial purpose or effect.[299]

An example of an unlawful effort to drive out troublesome competitors and control the labor market can be seen in *Radovich v. National Football League*.[300] In that case, the plaintiff football player had signed a contract with one NFL team, but asked to be traded to another NFL team after his contract expired. The first team's owner refused, so the player signed with a team in the rival All-America Football Conference (AAFC). The NFL then put the player on a five-year blacklist.[301] The Supreme Court held that the player had properly stated a Sherman Act claim because the conspiracy among the NFL and team owners inhibited players from transferring to other teams and thus had an anti-competitive effect on the labor market for football players.[302]

Similarly, in *Quinonez v. National Association of Securities Dealers, Inc.*, a securities sales representative was hired and then fired by two large securities dealers. Subsequently, no other securities firm would hire him. [303] The sales representative claimed that no firm would hire him "because of a boycott growing out of the express or tacit agreement that one member firm would not hire a person who had either been rejected or discharged by another

297. Edelman, *supra* note 296, at 640.

298. *Id*. at 640–41.

299. WILLIAM M. HANNAY, DESIGNING AN EFFECTIVE ANTITRUST COMPLIANCE PROGRAM § 1:43 (2019–20).

300. 352 U.S. 445 (1957).

301. *Id.* at 448.

302. Id. at 447. A more recent example is Colin Kaepernick's claim that the NFL and its owners have colluded to blacklist him for having instigated player protests during pregame performances of the national anthem. Kaepernick's claim, however, is a contract claim brought under the collective bargaining agreement between the NFL and the NFL Players' Association, rather than a statutory antitrust claim. The arbitrator rejected the NFL's equivalent of a 12(b)(6) motion to dismiss, and set the case for hearing. Ken Belson, *Colin Kaepernick's Collusion Case Against the N.F.L. Will Advance*, N.Y. TIMES (Aug. 30, 2018), https://www.nytimes.com/2018/08/30/sports/colin-kaepernick-collusion-case-nfl.html [https://perma.cc/T6U4-VEH2].The case settled in February 2019. Kevin Draper & Ken Belson, *Colin Kaepernick and the N.F.L. Settle Collusion Case*, N.Y. TIMES (Feb. 15, 2019), https://www.nytimes.com/2019/02/15/sports/nfl-colin-kaepernick.html [https://perma.cc/8K5Q-5L9K]

303. 540 F.2d 824, 826 (5th Cir. 1976).

member firm."[304] The Fifth Circuit held that the sales representative had stated a per se claim for relief under antitrust laws.[305]

Rule of reason analysis is usually applied to employee blacklisting if there are pro-competitive reasons for refusing to hire the employee and/or the restrictions on competition are unclear.[306] For example, when a basketball player was boycotted (pursuant to league rules) for gambling on the outcome of games, a federal district court refused to apply a per se test, because there were salutary procompetitive effects of ridding the sport of corrupt players.[307] Note that under a rule of reason analysis, the court focuses on whether the labor market is harmed and what the impact on competition is, not on the harm to the individual employee.[308]

On the other hand, a per se test has been applied to some employee boycott situations.[309] For example, a Georgia federal court applied the per se test when a golf association board consisting entirely of competing golf players suspended another player on a whim.[310] However, courts have held that the per se test does not apply if the governing body has a need for self-regulation and regulation is conducted according to due process principles,[311] and application of the per se rule to cases arising in the sports industry have been called into question in more recent cases.[312]

Regardless of whether the per se or rule of reason standard applies, to constitute an antitrust violation, there must be some indication that the employers *agreed*, even implicitly, to blacklist employees. While AI makes the collection, analysis, storage, and sharing of employee characteristics easy, it does not automatically lead to an antitrust violation. If employers using AI gather data either collaboratively or via a third party (such as an HR services provider) but make independent decisions based on the information, the conspiracy or collaboration element will be lacking. Thus, for example, if an HR service provider gave multiple companies underlying information

304. *Id*.

305. *Id.* at 830–31. Note that the facts of this case are likely sufficient to confer standing under section 4 of the Clayton Act. *See* Robert S. Chaloupka, *Antitrust Standing of Terminated Employees*, 138 ANTITRUST COUNS. §II(A) (2006).

306. WILLIAM T. LIFLAND, STATE ANTITRUST LAW § 3.06 (2019); Booker, *supra* note 234, at 35–36; David K. Haase & Darren M. Mungerson, *Agreements Between Employers Not to Hire Each Other's Employees: When Are They Enforceable?*, 21 LAB. LAW. 277, 283–84 (2006).

307. Booker, *supra* note 234, at 35–36 (citing *Molinas v. National Basketball Association,* 190 F. Supp. 241 (S.D.N.Y. 1961)).

308. Haase & Mungerson, *supra* note 306, at 283.

309. Booker, *supra* note 234, at 35 (citing Consol. Express Inc. v. N.Y. Shipping Ass'n, 602 F.2d 494 (3d Cir. 1979), *vacated*, 448 U.S. 902 (1980); Baughman v. Cooper-Jarrett, 391 F. Supp. 671 (W.D. Pa. 1975)).

310. *Blalock v. Ladies Prof'l Golf Ass'n*, 359 F. Supp. 1260, 1265–66 (N.D. Ga. 1973).

311. Daniel Fiorenza, *Blacklisted: Safe Sport's Disciplinary Policy Restrains A Coach's Livelihood*, 27 MARQ. SPORTS L. REV. 113, 124 (2016) (citing Denver Rockets v. All-Pro Mgmt, Inc., 325 F. Supp. 1049, 1064–65 (C.D. Cal. 1971)).

312. *See id.* at 126 (citing U.S. Trotting Ass'n v. Chi. Downs Ass'n, 665 F.2d 781, 790 (7th Cir. 1981); Brant v. U.S. Polo Ass'n, 631 F. Supp. 71, 78 (S.D. Fla. 1986)).

about a worker's disciplinary history aggregated from multiple sources, and each company made an individual decision of whether or not to hire the worker based on that and other information, under current law there would probably not be a violation. The information sharing would cross the line, however, if employers, either directly (such as through an industry association) or indirectly (through an HR provider) agreed on what characteristics would disqualify a worker from further consideration.

Additionally, even if there were an agreement not to hire certain types of individuals, if it embodied a procompetitive purpose, courts may find no antitrust violation. Thus, employers may be within their rights to agree not to hire an employee shown to be in violation of industry rules or ethics.[313] For example, employers might agree not to hire employees in continual violation of safety standards, or an accountant with a history of embezzlement, or a nurse with a history of opioid theft.

In addition to the federal antitrust laws, some states have statutes[314] prohibiting the blacklisting of employees.[315] These statutes can be either criminal and civil just civil.[316] Some states provide a safe harbor for truthful job references, however,[317] and it is possible that some gathering and disseminating of AI-gathered data may fall within the safe-harbor exceptions. For example, if an HR service provider uses AI to scour the web for data of misconduct, illegalities, drug use, sexual improprieties, or other improper conduct by a job applicant, or aggregates such information from its various clients, that might likewise fall into a safe harbor exception.

In sum, employer information-sharing, no-poaching agreements, and blacklisting can violate the antitrust laws, and the use of AI makes such violations more likely than in the past by making information about employees easier to amass and transmit. Moreover, the use of AI by HR companies can make the sharing of information difficult to detect because comparative data is often built into the algorithms. Therefore, it may be necessary to revise some of the doctrines in our antitrust laws to make it clear that antitrust laws apply to the anti-competitive potential that stems from the use of AI in the workplace. It may also be appropriate for the FTC to initiate administrative actions similar to the hearings it held in 2018 on the antitrust implications of pricing algorithms.[318]

---

313. *See, e.g.*, DOJ/FTC Guidelines, *supra* note 266 (noting that "a trade association may help establish industry standards that protect the public. . . .").

314. *See, e.*g, ALA. CODE § 13A-11–123 (1975); ARIZ. REV. STAT. ANN. §§ 23-1361 to -1362 (2019) (effective until June 30, 2020); CAL. LAB. CODE §§ 1050–1053 (West 2019); COLO. REV. STAT. §§ 8-2-110 to -114 (2019); CONN. GEN. STAT. § 31–51 (2019).

315. Lifland, *supra* note 306; *see generally* Edward M. Cramp, Annotation, *Validity, Construction, and Operation of State Blacklisting Statutes*, 95 A.L.R. 5th 1 (2002). A list of these statutes can be found at 1 POLICIES AND PRACTICES (HR SERIES) § 60:2 (2019).

316. *See generally* Cramp, *supra* note 315.

317. *Id.* at § 2(a), 10.

318. *See Deep Dive*, *supra* note 250 and accompanying text.

D. Labor Law Issues

In addition to issues AI poses under discrimination, privacy, and antitrust laws, there are also several labor law issues that can arise from the use of AI in the workplace. First, there is a question of whether electronic monitoring and surveillance violates employees' fundamental right, under the labor laws, to engage in concerted activity for mutual aid and protection. Second, where unions exist, do they have a right to bargain about the use of AI in the workplace or to acquire information about the installation and use of AI in HR decisions? Third, how does the use of AI surveillance and algorithmic decision-making affect the ability of unions to represent employees effectively in the grievance procedure and in collective bargaining? These are discussed below.

1. AI and Concerted Protected Activity

The core provision of the National Labor Relations Act is Section 7, which creates a right for employees to engage in "concerted activit[y] for . . . mutual aid or protection."[319] Section 7 has been interpreted by the Supreme Court and the National Labor Relations Board (N.L.R.B.), the agency that administers the statute, as protecting employees from dismissal or other sanctions when they engage in any collective action with the aim of improving their position as employees. Section 7 ensures employees are free to discuss their working conditions together and determine whether they wish to engage in collective bargaining. Working conditions includes the topics of wages, hours, benefits, safety conditions, employment policies and practices, supervisors, and in some cases, customers or clients.[320] Moreover, it is well-settled that Section 7's protection applies broadly to actions undertaken by two or more employees, and to actions taken by an individual acting alone in an effort to induce others to form a union, organize or participate in workplace protests, or otherwise attempt to apply concerted pressure on an employer to achieve a work-related goal.[321] Thus, if an employer penalizes or attempts to intimidate an employee for advocating collective action around workplace issues, , it violates the labor law.[322] Moreover, an action by an employer that restricts or "chills" these activities is an unfair labor practice. For example, an employer social media policy that prohibits employees from using Facebook to complain among themselves about their work would violate Section 7, as would any employer search of its employees' social

319. National Labor Relations Act (NLRA), 29 U.S.C. § 157.

320. *See* George H. Pike, *Social Media and the Workplace*, INFORMATION TODAY, Nov. 2014, at 1, 2.

321. *See, e.g.*, N.L.R.B. v. City Disposal Syss., Inc., 465 U.S. 822 (1984).

322. Eastex, Inc. v. N.L.R.B., 437 U.S. 556, 563–70 (1978).

media sites to ascertain whether one or more employees is engaged in union activity. [323]

There are many ways in which employees' Section 7 rights can come into conflict with employer efforts to collect data for developing or implementing AI-enabled personnel management by means of monitoring and surveillance. For over a hundred years, employers have attempted to monitor their employees to deter collective action and to identify and weed out "trouble-makers."[324] They have used company spies and hidden cameras, and inserted infiltrators into employee groups in order to detect and deter employees' collective action.[325] With the enactment of the NLRA in 1935, these and other employer surveillance tactics have frequently been challenged as interfering with employees' Section 7 rights.

The N.L.R.B. has held that it violates the statute for an employer to engage in surveillance or create the impression of surveillance in order to detect and suppress of employees' protected Section 7 activities. Thus, for example, it is unlawful for a supervisor to observe employees attending a union meeting at the union hall to vote on whether or not to strike.[326] The test is "whether the employee would reasonably assume . . . that their [sic] union activities had been placed under surveillance."[327]

Of course, not all information gathering by employers is unlawful. Employers have many legitimate reasons to monitor their workers. For example, they may want to monitor workers' locations in order to prevent loitering on the job ("stealing time") or to make sure employees are not engaged in forbidden conduct, such as pilfering, stealing trade secrets, watching pornography while at work, and so forth. They also might monitor for safety reasons—to ensure employees are not entering hazardous areas or to prevent strangers from entering the workplace. Employers also might want to monitor employees' work so they can reward exceptional performance, promote greater effort, or track individual improvement. When the surveillance has a legitimate purpose, but also has the potential to observe or chill protected collective action, the N.L.R.B. considers whether the employer's legitimate purpose is outweighed by the burden the specific means utilized places on employees' Section 7 rights.[328]

---

323. *See* Christine N. O'Brien, *The First Facebook Firing Case Under Section 7 of the National Labor Relations Act: Exploring the Limits of Labor Law Protection for Concerted Communication on Social Media*, 45 SUFFOLK U.L. REV. 29, 32, 35 (2011) (discussing settlement of case involving employee who had posted remarks on Facebook angrily implying that her supervisor was mentally ill and disparaging him with expletives).

324. *See* sources cited *supra* note 95.

325. *Id.*

326. Ivy Steel & Wire, Inc., 346 N.L.R.B. 404, 404 (2006).

327. *Id*.

328. *Compare* S.J.P.R., Inc., 306 N.L.R.B. 172, 172 (1992) (finding surveillance unlawful because it "constituted more than ordinary or casual observation" and there was no evidence of "safety or property" concerns) *with* Halo Lighting Div. of McGraw Edison Co., 259 N.L.R.B. 702, 716 (1981) (finding

One frequently challenged form of surveillance involves polling of employee attitudes. Since the 1920s, employers have conducted polls of their workers to determine whether there are morale problems and to get suggestions for improvement.[329] While these are legitimate and lawful purposes, when the purpose of a poll is a disguised effort to determine which employees are likely to support a union drive, or to intimidate potential union supports into silence or inactivity, it will be found to be unlawful.[330] In fact, the N.L.R.B. has gone beyond explicit polls; it has found a violation when an employer action forces an employee to make an "observable choice" or otherwise publicly display their support or opposition to a union.[331]

Another common form of employer surveillance is the use of hidden cameras. Employers often install cameras to prevent pilferage or shirking on the job. Cameras can also identify hazardous conditions and facilitate proactive safety interventions. These concerns are legitimate and do not violate the statute. However, surveillance cameras can also spy on employees' organizing activities, picket lines, or other protected conduct. As a result, the N.L.R.B. has considered when the use of overt and hidden surveillance cameras interferes with employees' rights to engage in concerted activity for mutual aid and protection. In several cases, the N.L.R.B. has held that "absent legitimate justification, an employer's photographing of its employees while they are engaged in protected concerted activities constitutes unlawful surveillance."[332] However, it has also held that it is lawful for an employer to photograph or videotape certain activities outside his plant without violating the Act "where he can establish a legitimate purpose for this activity."[333]

To determine the lawfulness of a particular instance of surveillance, the N.L.R.B. considers whether the employer has used surveillance to target a specific individual suspected of union activity, or whether an employer has

---

surveillance lawful because of the "possibility of violence" and the fact that an altercation had already occurred).

329. Sanford M. Jacoby, *Employee Attitude Surveys in Historical Perspective*, 27 INDUS. RELS. 74, 75 (1988).

330. *See, e.g.*, Struksnes Constr. Co., 165 N.L.R.B. 1062 (1967) (articulating test for determining whether polling is unlawful effort to intimidate employees).

331. *See, e.g.*, Allegheny Ludlum Corp., 333 N.L.R.B. 734, 745 (2001), *enforced*, 301 F.3d 167 (3d Cir. 2002) ("[The employer] violated Section 8(a)(1) by approaching individual employees and asking them to consent to be filmed for the purpose of a campaign videotape, and by requiring employees to register an objection with an agent of [Allegheny Ludlum] in order to avoid being included in its campaign videotape" because the request "forced employees to make an observable choice that demonstrates their support for or rejection of the union.") (internal quotation marks and citation omitted).

332. Brunswick Hosp. Ctr., Inc., 265 N.L.R.B. 803, 807 (1982); U.S. Steel Corp., 255 N.L.R.B. 1338, 1338 (1981); *accord* Dynatron/Bondo Corp., 323 N.L.R.B. 1263, 1269 (1997); Glomac Plastics, Inc., 234 N.L.R.B. 1309, 1320–21 (1978); Larand Leisurelies, Inc., 213 N.L.R.B. 197, 207 (1974); Flambeau Plastics Corp., 167 N.L.R.B. 735, 743 (1967).

333. Lechmere, Inc., 295 N.L.R.B. 92, 99–100 (1989) (finding no violation when employer installed rotating cameras outside its store in order to deter illegal activity in the parking lot and apprehend shoplifters).

changed its level and type of surveillance in light of a union drive.[334] The N.L.R.B. has stated that "[a]lthough an employer may observe open union activity on or near its property, an employer may not do something 'out of the ordinary' to give employees the impression that it is engaging in surveillance of their protected activities."[335]

In the late twentieth century, employers began to use GPS tracking devices on vehicles to monitor their workers' on-the-job activities. The trackers indicated whether workers were wasting time and whether they were meeting productivity standards.[336] Although GPS tracking devices were resisted by drivers and opposed by unions on the grounds they were intrusive and oppressive,[337] such devices were usually found to not be unreasonable impingements on Section 7 activities in nonunion workplaces.[338] However, the N.L.R.B. concluded that the use of such devices does interfere with Section 7 rights when it is used to track the movements of specific individuals involved in organizing campaigns.[339] Moreover, the N.L.R.B. also held that in the presence of a union, the installation of GPS can constitute a change in working conditions that is subject to a mandatory bargaining obligation.[340]

Today's methods of surveillance are an even greater threat to workers' Section 7 rights than old-fashioned polls, cameras, or even basic GPS trackers. Electronic badges, cell phone applications, RFID, wearable devices and other AI-enhanced surveillance devices can be used for legitimate purposes such as to improve productivity or prevent theft, but they can also

334. *See, e.g.*, Caterpillar Inc., 322 N.L.R.B. 674, 683–84 (1996) (holding no violation where a supervisor watched over the shop floor from his normally assigned work area in order to make sure everything was running smoothly and incidentally observed organizing activity).

335. Sprain Brook Manor Nursing Home, 351 N.L.R.B. 1190, 1191 (2007); *Cf.* Intertape Polymer Corp., v. N.L.R.B., 801 F.3d 224, 234–41 (4th Cir. 2015) (finding no violation when employer had a legitimate reason to be present at the location where it observed the employees' union activities); Aladdin Gaming, LLC, 345 N.L.R.B. 585, 585–87 (2005) ("A supervisor's routine observation of employees engaged in open Section 7 activity on company property does not constitute unlawful surveillance.").

336. NAT'L WORKRIGHTS INST., ON YOUR TRACKS: GPS TRACKING IN THE WORKPLACE 6–7 (reporting widespread use of GPS on commercial vehicles by employers by early 2000s), https://epic.org/privacy/workplace/gps-traking.pdf [https://perma.cc/T8JG-M66V].

337. *See, e.g.*, *id.* at 10 (describing protest action by snowplow drivers in Massachusetts after their employer instituted requirement that they carry GPS-enabled cell phones to monitor their speed).

338. *See e.g.*, CSC Holdings, L.L.C., No. 29-CA-190108, 2018 WL 2003170 (N.L.R.B. Div. of Judges) (April 27, 2018) (finding no violation for installation of a GPS tracker in vehicles of sales representations because they have no expectation of privacy in the company's equipment).
(finding no violation for installation of a GPS tracker in vehicles of sales representations because they have no expectation of privacy in the company's equipment).

339. N.L.R.B., Advice Memo. on East Coast Mech., No. 22-CA-253245 (Feb. 6, 2003).

340. N.L.R.B., Advice Memo. on BP Expl. Of Alaska, Inc., Case 19-CA-29566 (July 11, 2005) (imposing obligation to bargain with union over employer unilateral installation of GPS monitoring in trucks). *See also* Great Western Produce, Inc., 299 N.L.R.B. 1004, 1024 (1990) (holding that the unilateral implementation of certain work rules, including a record-keeping system that tracked employees' shortcomings, violated section 8(a)(5)). *But see* N.L.R.B., Advice Memo. on Roadway Express, Inc., Case 13-CA-39940 (Apr. 15, 2002) (concluding there was no duty to bargain over employer's unilateral implementation of GPS system because drivers were already required to maintain constant contact with dispatchers via two-way radio, so the new system was not a significant change in working conditions.)

be used to listen to employees' conversations, record employee movements, monitor biological reactions, and identify participants in employee gatherings. These uses enable an employer to pinpoint union supporters and intimidate others.

As explained above, the N.L.R.B. has maintained that surveillance, or creating an impression of surveillance, is an unlawful interference with Section 7 rights unless there is a legitimate justification that outweighs the coercive nature of the surveillance. However, the standard begs the question of what constitutes legitimate justification and how to weigh the factors when the N.L.R.B. engages in balancing. In the era of AI and management analytics, it remains to be seen whether and to what extent employers' detailed data collection about their employees' whereabouts, conversations, social networks, off-work activities, personal habits, interests, proclivities and moods are found to be labor law violations. After all, a device that listens in on conversations can pick up union talk more effectively than can any company spy. Moreover, an AI algorithm that uses biomarkers and body language to identify which employees are dissatisfied at work can predict which ones are likely to become union supporters or simply troublemakers. These uses of electronic monitoring surely pose a danger to workers' Section 7 rights.

To date there have been no cases considering when the use of advanced monitoring and AI, even for legitimate efficiency purposes, run afoul of the labor laws. However, there are some cases that bear on a related issue: whether employer can monitor employee emails, social media postings, and other online activities inside or outside of the workplace.

In November 2010, the N.L.R.B. brought a charge against an employer for firing an employee who had disparaged her supervisor on her Facebook page.[341] The N.L.R.B. maintained that the posting was concerted protected activity under the labor law. While this case was ultimately settled, the N.L.R.B. has, until recently, continued to maintain that social media postings by employees are protected activities with which an employer cannot interfere absent significant justification. For example, in 2015, the N.L.R.B. held that an employer cannot maintain a policy that places limits on employees' ability to discuss the company on social media. In *Boch Imports,* it stated that

[T]he [company's] social media rule required employees to identify themselves when posting comments about the Respondent, the Respondent's business, or a policy issue. This rule was overly broad, because employees would reasonably construe it to cover comments about their terms and conditions of employment, and the self-identification requirement reasonably

341. *See* David L. Bayer, *Employers Are Not Friends With Facebook: How the N.L.R.B. Is Protecting Employees' Social Media Activity*, 7 BROOK. J. CORP. FIN. & COM. L. 169, 174 (2012).

would interfere with their protected activity in various social media outlets.[342]

However, the lawfulness of employer monitoring of employee online activity is currently in flux. Since April 2018, the five member N.L.R.B. has had a majority of Republican members, with three members having been appointed by President Donald Trump.[343] Accordingly, the scope of lawful employer surveillance has widened. In particular, two recent decisions suggest that the N.L.R.B. may soon reverse its position and may instead be moving in the direction of permitting employers to restrict and monitor employee electronic communications.

In 2014, the N.L.R.B. held in *Purple Communications* that employers cannot bar employees from using a company email system for nonwork related purposes, including union communications.[344] The decision was heavily criticized by employers, and on August 1, 2018, the Trump Board announced that it was reconsidering the decision. In *Caesars Entertainment Corp.,* the N.L.R.B. invited all interested amici to submit briefs on the questions of whether *Purple Communications* should be overruled, what the standard for employers' regulation of employee email and other electronic communication should be, and whether the standard it adopts should also apply to regulation of employees' use of instant messages, texts, postings on social media.[345] Most commentators believe the call for briefs signifies a major retreat in the N.L.R.B.'s policing of employers' electronic communications policy, at least in the workplace.

The N.L.R.B.'s call for reconsideration of *Purple Communications* follow on its decision, issued on December 14, 2017, in *Boeing Corp*., where it held that an employer can maintain a no-camera rule, including a prohibition on cell phones, in its premises even if the rule interferes with and/or is likely to chill employees' protected activity.[346] In *Boeing*, the N.L.R.B. expressly overruled a 2004 precedent in which the N.L.R.B. announced it would analyze employer rules that affect employee exercise of Section 7 rights under a standard that considered whether "(1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights."[347] The N.L.R.B. went

342. Boch Imports, Inc., 362 N.L.R.B. 706, 707 (2015), *aff'd*, 826 F.3d 558 (1st Cir. 2016).

343. *Members of the N.L.R.B. Since 1935*, NATIONAL LABOR RELATIONS BOARD, https://www.N.L.R.B..gov/about-N.L.R.B./who-we-are/board/members-N.L.R.B.-1935 [https://perma.cc/5PP4-LSWA] (last visited Oct. 21, 2019).

344. Purple Communications, 361 N.L.R.B. 1050, 1050 (2014).

345. Case 28-CA-060841, 2018 WL 3703476 (N.L.R.B.) (Aug. 1, 2018).

346. The Boeing Co., 365 N.L.R.B. No. 154, at *19 (Dec. 14, 2017). It stated that "We find that any adverse impact of Boeing's no-camera rule on the exercise of Section 7 rights is comparatively slight and is outweighed by substantial and important justifications associated with the no-camera rule's maintenance."

347. *Id.* at 24 (quoting Lutheran Heritage Village — Livonia, 343 N.L.R.B. 646, 647 (2004)).

beyond approving the employer's no-camera rule to state that an employer is permitted to maintain a rule that requires employees to engage in "harmonious interactions and relationships" and maintain "respect and civility," even if such a rule could prevent employees from criticizing the employer and organizing opposition. A dissent by Member McFarren pointed out that "civility rules" were not at issue in the case, and that, moreover, such rules are often understood by employees to bar them from engaging in union organizing, strikes, and other protected conduct. He stated,

> Our experience demonstrates, moreover, that the fear of reprisal that is instilled in employees by overbroad "civility rules" is well-founded. The cases in which employers have applied such rules to discipline or discharge employees for engaging in protected concerted activity are numerous. These cases confirm the tendency of employers to interpret overbroad and ambiguous civility rules to prohibit conduct that is clearly protected under the Act.[348]

Caesars Entertainment Corp. and the *Boeing Corp*. case suggest that the current N.L.R.B. is likely to approve of employers' use of extensive monitoring of employees' online and electronic communications in order to police the newly authorized civility rules. If so, the labor law will be no barrier to extensive monitoring and surveillance of employees' online activities, monitoring that could be used to amass data for use in AI enabled employee assessments.

2. The Duty to Bargain over AI and Electronic Surveillance

Under the labor law, when a union is certified as a representative of a majority of a bargaining unit the employer has an obligation to bargain with it over wages, hours, and working conditions.[349] In addition, an employer cannot make a unilateral change in existing wages, hours, and working conditions without first bargaining with the union to the point of impasse.[350] These principles have important implications for the implementation of AI in the unionized workplace.

---

348. Member McFarran, dissenting, also stated:

> First, the majority makes no genuine attempt to *define* the "basic standards of civility." What are those standards—and what are they, in particular, in a workplace setting? Are they really the same, moreover, in every workplace setting? The same on a construction site as in a hospital? The same on a loading dock as in a retail store? Second, the majority seems oblivious to the possibility that common forms of protected concerted activity under the National Labor Relations Act may reasonably be understood as uncivil. Does walking off the job to protest unsafe working conditions conform to "basic standards of civility"? Or distributing literature that, in impolite language, criticizes an employer's failure to pay employees what they are owed and urges employees to resist? The majority's apparent decision to permit all employers to maintain whatever "civility" rules they wish simply ignores the reality of the labor disputes that can arise in various workplaces and move employees to act to defend themselves—just as federal labor law aims to encourage.

Id. at *39.

349. 58 U.S.C. 158(a)(5) (2012).

350. N.L.R.B. v. Katz, 369 U.S. 736, 745 (1962).

As explained above, an employer has considerable latitude to engage in surveillance and monitoring if it does so for a legitimate purpose. That said, once there is a union certified, an employer must bargain with a union about the use and placement of surveillance cameras.[351] In addition, the installation of GPS trackers can be considered a change in working conditions that is subject to a duty to bargain. Logically, the same rationale would apply to the installation of other trackers and bio-monitors, so that they too would subject employers to a bargaining obligation. In those instances, an employer would be required to bargain with the union prior to implementing AI related monitoring.

For example, in *Chemical Solvents, Inc.*,[352] an employer installed surveillance cameras to which a union objected. The N.L.R.B. ruled the employer violated the duty to bargain by installing the cameras without first bargaining with the union. It explained:

> It is difficult to accept the proposition that cameras clearly visible to employees are of less concern to employees than hidden ones or would have less potential impact on their working environment. Indeed, the contrary could be argued. The placement of at least some of the cameras resulted in their viewing areas of the facility regularly used by employees. I do not dispute the Respondent's contention that the new cameras comported with DHS' suggested security measures. However, the Respondent has not shown that DHS required the particular number of new cameras or their particular locations. Those matters aside, other issues also could have been raised or discussed during bargaining, such as the size of the cameras or how their purpose could be best communicated to employees. I cannot, therefore, accept the Respondent's summary conclusion that "[b]argaining would have been futile and unproductive."[353]

The cases supporting a bargaining obligation for surveillance cameras and GPA trackers may not apply to all types of electronic monitoring, for two reasons. First, there is only a bargaining obligation if the devices are found to be "mandatory subjects of collective bargaining."[354] The N.L.R.B. and the Supreme Court have stated that not all matters of concern to employees are subject to "mandatory bargaining," and specifically that employers have no duty to bargain about "managerial decisions, which lie at the core of entrepreneurial control.[355]" While the N.L.R.B. has found that the installation of GPS trackers and cameras are a mandatory subject of bargaining, the issue of other monitoring devices is as yet an open question.

---

351. In *Colgate-Palmolive Company*, the Board held that an employer must bargain with a union over the placement of hidden surveillance cameras because the use of such cameras is germane to the working environment and not within management's core entrepreneurial concerns. 323 N.L.R.B. 515 (1997). *Accord*, Nat'l Steel Corp., 335 N.L.R.B. 747 (2001).

352. 362 N.L.R.B. 1469, 1503 (2015).

353. *Id*.

354. N.L.R.B. v. Wooster Div. of Borg-Warner Corp., 356 U.S. 342, 348 (1958).

355. Fibreboard Paper Prods. v. N.L.R.B., 379 U.S. 203, 223 (1964) (Stewart, J., concurring).

Second, even if such devices are determined to be subjects of mandatory bargaining, the duty to bargain only requires an employer to refrain from introducing them until it has bargained with a union until impasse. Once impasse is reached, the employer is permitted to implement its proposed changes.[356] Thus the duty to bargain gives the union the leverage of delay and the right to information, but it does not preclude the installation of the devices altogether.

Another issue that is sure to arise is whether an employer must bargain about the use of AI algorithms to guide it in decisions concerning discipline, job assignment, or promotion. There would also be a related issue about employees' rights to see and contest the conclusions of any AI-enhanced personnel information. For these questions, as with the installation of electronic monitoring devices, the outcome would turn on whether these issues are subjects of mandatory bargaining.[357]

E. Union Representation in the Era of Algorithmic Decision-Making

Unions represent employees both in the handling of grievances and in the negotiation of agreements. In both capacities, they need access to information gleaned by electronic monitoring and to the process by which AI is implemented in employer decision-making.

The Supreme Court has held that a union has a right to information necessary for it to participate in meaningful bargaining.[358] In order to trigger a bargaining obligation, the union must request the information, and it must show that the information is relevant and necessary for the union to raise and discuss intelligently the issue in bargaining.[359] A corollary of the employer's duty to bargain over installing electronic surveillance and using AI in employee evaluation and discipline is a duty to provide a union with information about an employer's practices and prospective plans regarding the use of AI for personnel management decisions for the purposes of bargaining. With such information, a union could bargain for transparency about the use of AI and place some limits on the extent and uses of surveillance.

As with bargaining, unions also need access to AI information in order to effectively represent employees in the grievance procedure. When electronic monitoring and AI algorithms are used to detect employee

356. N.L.R.B. v. Katz, 369 U.S. 736, 741 (1962).

357. A detailed discussion of the factors determining what issues are subjects of mandatory bargaining and which are not is beyond the scope of this paper. However, it bears noting that the standard is often elusive and the decisions are hotly contested. *See, e.g.*, First Nat'l Maint. v. N.L.R.B., 452 U.S. 666, 686 (1981) (finding no duty to bargain about an employer's decision to close part of its operation once a union was certified).

358. N.L.R.B. v. Truitt Mfg. Co., 351 U.S. 149, 152 (1956).

359. N.L.R.B. v. Whitin Machine Works, 217 F.2d 593, 594 (1954). *See also* S.L. Allen & Co., 1 N.L.R.B. 714, 728 (1936).

misconduct, a union representing the employee will seek to refute the charges or mitigate the punishment. For example, nearly all collective bargaining agreements restrict an employer's right to dismiss a worker to situations where it has "just cause" to do so. The just cause standard is vague and open-ended, and cases are often decided by an arbitrator. However, to determine whether there has been just cause, a union needs to know what informed a decision that is in dispute. An employer might decide to terminate an employee whose productivity is below average on the grounds that it does not believe that the employee will not improve. The prediction might be the result of an AI assessment of the employee's past and present biological markers and emotional states. The union would need to understand how all these factors fit into the assessment in order to effectively counter it.

The Supreme Court has held that union representatives are entitled to relevant information to enable them to perform their function in the grievance procedure.[360] Thus, presumably, an employer who based a disciplinary action against an employee on the ground that a company rule was breached where it learned of the breach from a GPS device, an electronic listening device, a hidden camera, or a behavior monitor, would be required to reveal how the rule infraction was discerned. Moreover, if an employer based a disciplinary decision on the conclusion of an AI algorithm, that too would have to be revealed.

Although there is, to date, no case directly on point, there is some case law on a related issue that supports the conclusion that the duty to provide information includes a duty to reveal electronic monitoring. In *Michigan State Employees Ass'n*,[361] the employer installed a new voicemail system. The union, COSA, learned that it was telling callers that their telephone conversations might be recorded. Because the collective-bargaining agreement between the employer and COSA allows employees to use the employer's telephones and email for union business, COSA submitted an information request asking when the employer began using this recorded telephone greeting, whether it monitored employee email communications, and, if so, when it began doing so, and which employees' email had been monitored. It also asked for the employer's rationale or business necessity for monitoring emails, and for any written communications sent to employees advising them that their email might be monitored. The president, Moore, replied by letter, but failed to provide the date when the phone system began advising callers that their conversations could be monitored and refused to provide information about whether it monitored employees' email. Instead, Moore's letter stated that "[t]he computers and MSEA.org email domains are the property of MSEA and the Employer is well within its Management rights." The union brought an unfair labor practice proceeding

360. N.L.R.B. v. Acme Indus. Co., 385 U.S. 432, 436–38 (1967).

361. 364 N.L.R.B. No. 65 (Aug. 4, 2016).

at the N.L.R.B., challenging the failure to provide the information. The N.L.R.B. ruled that the union was entitled to the information it had requested and that employer acted unlawfully when it refused to do so. It explained that:

> [E]ven if . . . Respondent owned the computers which the employees used and. . . . [e]ven assuming . . . that. . . Respondent was 'within its Managements' when it installed the electronic equipment, a right to make a unilateral change in a condition of employment doesn't affect either the union's entitlement to information about the change or the employer's duty to provide that information.[362]

In a similar vein, the N.L.R.B. has held that an employer cannot resist an information request concerning its disciplinary actions on the grounds that the request is too burdensome. Rather, the N.L.R.B. takes the position that a union needs such information in order to evaluate the strength of any employee's grievance and determine whether or not to pursue it, thereby eliminating frivolous claims at an early stage.[363] Hence it is fair to conclude that unions are entitled to information about the use of AI and the results of electronic monitoring when the information is germane to a specific grievance.

Obviously, obtaining information does not guarantee success in the grievance procedure. To be effective, unions need to be able to interpret, evaluate, and refute the conclusions drawn from AI- enhanced decision-making. To do so, unions need more than the algorithm and the raw data—they need to understand how the algorithm works and what information is used and excluded in reaching its conclusion. For this, they may need to hire experts in AI and computer engineering to assist with grievance handling and bargaining preparations. Unions have a long history of utilizing experts, such as economists to evaluate employer wage concession demands or industrial hygienists to monitor workplace health and safety conditions.[364] In the world of management by AI, it would be appropriate and necessary for unions to turn to AI experts to assist them in protecting workers rights and defending workplace justice in the evolving world of people analytics.

IV. POLICY PRESCRIPTIONS AND AGENDA FOR FUTURE RESEARCH

Employers and HR services providers today are gathering, analyzing, and using huge quantities of data to screen potential new hires, monitor

362. *Id.*

363. Pfizer, Inc., 268 N.L.R.B. 916, 918 (1984), *enf'd*, 763 F.2d 887 (7th Cir. 1985).

364. *See, e.g.*, *William E. Spriggs, Chief Economist to AFL-CIO*, AFL-CIO, https://aflcio.org/policy-experts/william-e-spriggs [https://perma.cc/BH4Y-JSVP] (last visited Oct. 21, 2019) (biography of William E. Sprigg, former Chair of the Economics Department at Howard University); *Peg Seminario, Director of Occupational Safety and Health at AFL-CIO,* AFL-CIO (biography of Peg Seminario, Master in Public Health from Harvard University), https://aflcio.org/policy-experts/peg-seminario [https://perma.cc/P8JA-ASTN] (last visited Oct. 21, 2019).

existing workers, and hiring, discipline, and firing decisions. Literally dozens of companies have been created in the past five years to provide such services to employers.[365] Yet the field is only in its infancy. Its true impact will not be felt for another several years, until these companies will have gathered enough data on enough workers to be able to predict reliably the future behavior of applicants and existing workers on an individualized basis. By that point, job interviews, resumes, and work histories may well be irrelevant, because employers will have access to datasets from an individual's past work history that can be mined to identify or predict not only performance history, but also things like race, union proclivity, work ethic, personality, political affiliation, employer loyalty, and future health care costs.

Both gathering and using such data have enormous implications for the application of existing workplace laws, yet are occurring with no legal or regulatory oversight. Perhaps existing laws will be sufficiently adaptable to respond to these new conditions, but there is significant risk they will not.[366] Moreover, given the blinding pace at which companies currently are collecting data on workers, a legal response may quickly become a moot point. Once sufficient data are collected, it likely will be difficult to put the genie back in the bottle.

This article discusses four different areas of law affecting the workplace that are particularly endangered by AI: anti-discrimination law, privacy law, antitrust law, and labor law. Of these, antidiscrimination law is the area that has, by far, received the most scholarly attention. Yet research to-date has focused almost exclusively on how AI might have a discriminatory effect on *hiring* decisions.[367] Much more research needs to be done on whether and how AI will have a discriminatory effect on monitoring, career-tracking, disciplining, and firing workers.

Additionally, Title VII and other antidiscrimination laws need to be interpreted or amended to protect workers from potential discrimination caused by the use of AI technology. For example, the law of disparate impact should be clarified to ensure that plaintiffs need to show, in their prima facie case, only that an algorithm *as a whole* caused a disparate impact; plaintiffs should not be expected to show precisely how the algorithm produced the bias. Similarly, after a plaintiff makes a prima facie showing, the burden should be squarely on the employer to reverse-engineer the algorithm, explain how it made its hiring recommendations, and demonstrate that each factor going into the recommendation is consistent with business necessity. Finally, standards should be set for auditing algorithms used in the hiring process to identify algorithm inputs and monitor algorithm outputs in order to ensure nondiscrimination.

---

365. *See supra* Part I.B.

366. Hirsch, *supra* note 6.

367. *See* articles cited in Part II.A.

The other areas of law have received little or no scholarly attention to date. As discussed in Part II.B, above, current American privacy laws give workers very little protection from collection and use of their personal and professional data. Moreover, there are many open questions that will define the scope of worker privacy rights, such as whether workers have an ownership interest in data compiled from or about them, whether and under what circumstances they can exclude others from seeing or using such data, whether they have a right to access the data, whether their data travel with them as a lifetime electronic resume that they can neither see nor rebut, and whether workers have recourse if their data is incorrect and is used in an adverse employment action or is shared with others.

The United States Congress should enact a national omnibus privacy statute, using the European General Data Protection Regulation (GDPR)[368] as a starting point but augmenting it to specifically address data collection in the employment context. The GDPR gives citizens of the European Union certain rights over their "personal data" — meaning "information that relates to an identified or identifiable individual" — that is collected or retained by others. Though the GDPR was not specifically aimed at data collected by AI, or data collected in the workplace, many of its provisions appear to apply in that context. Examples include the right to access personal data (Article 15), the right to correct erroneous data (Article 16), the right to be forgotten (Article 17, and the right not to be subject to a decision based solely on automated processing, including profiling (Article 22).[369] This latter right, if applied to the employment context, might prevent an employer from terminating a worker based solely on data obtained from AI surveillance.

Any statute enacted in the US should give workers the right to access to, and prevent the sharing of, personal employment-related data, including video-recorded job interviews, information gained through monitoring by previous employers, and personality tests. Additionally, the statute should restrict or require prior notice and consent for electronic monitoring and employer access to employees' social media accounts.

In the antitrust context, using artificial intelligence in the workplace may violate existing antitrust laws if data collected from multiple employers within an industry are used to blackball "undesirable" workers or to establish no-poaching agreements Moreover, it is likely to be found to be a violation if an algorithm uses industry-wide data to set salaries, or if an HR services provider uses data gathered from multiple companies to make hiring, salary, job classification, or other such employment-related decisions or recommendations. The antitrust laws should be interpreted to clarify that these all are forms of information sharing are prohibited conduct. The

368. Regulation 2016/679 of the European Parliament and the Council of 27 April 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, 2016 O.J. (L 119).

369. *Id*.

Federal Trade Commission is positioned to draw the line between permitted and prohibited conduct, such as the line between anticompetitive and procompetitive exchanges of salary or benefits information. The agency held hearings in 2018 on the use of algorithms to set consumer prices,[370] and these could provide a starting point for such regulation.

In the labor law context, AI raises fundamental questions about the ability of workers to engage in concerted activity for mutual aid and protection, whether unions have a right—and whether employers have a corresponding duty—duty to bargain about workplace monitoring and data collection, and the ability of unions to represent employees effectively in the grievance procedure or in collective bargaining. Future N.L.R.B. and court decisions should clarify that employer surveillance with the purpose or effect of chilling concerted activity is unlawful under Section 7. Similarly, Section 7 should be interpreted to prohibit employers from using electronic surveillance, biomarkers, keystroke/email surveillance software, or other monitoring technologies in ways that might identify current or potential union activity, or to mine social media for the same effect. Section 8(a)(5) should be interpreted to impose upon employers a duty to bargain with unions over the existence and scope of electronic monitoring and the use of algorithms in decisions involving discipline, job assignment, promotion, or pay. It should also ensure that unions and individual employees have the right to obtain and to contest data collected by AI. Finally, the existing duty on employers to provide unions with information necessary for meaningful bargaining and grievance-resolution should be extended to information about an employer's practices and plans regarding the use of AI in personnel management decisions, and to information about algorithms or data collected by AI that an employer has used in personnel decisions affecting individual grievants.

V. CONCLUSION

Today's workplace is transforming rapidly. Most visibly, workers report to a dizzying array of traditional employers, HR services providers, electronic work-distributing platforms, and customers. They perform work in offices, coffee shops, cars, and at home. Less visibly, companies are collecting unfathomable quantities of data on workers that will significantly tilt the balance of workplace power in favor of employers at workers' expense. We should not go down that path blindly.

370. *See supra* note 250 and accompanying text (discussing FTC hearings on pricing algorithms).