

COMMENTS OF THE KNOWING MACHINES RESEARCH PROJECT

Melodi Dincer,<sup>1</sup> Kate Crawford<sup>2</sup> & Jason Schultz<sup>3</sup>

to the

White House Office of Science and Technology Policy

RFI on Automated Worker Surveillance and Management

88 Fed Reg. 27,932

June 27, 2023

---

The Knowing Machines Research Project (Knowing Machines) submits these comments in response to White House Office of Science and Technology Policy’s (OSTP) May 3, 2023 Request for Information on Automated Worker Surveillance and Management (RFI).<sup>4</sup> In alignment with its 2022 Blueprint for an AI Bill of Rights, OSTP is considering the “prevalence, impacts, and deployment” of worker surveillance technologies and how Federal agencies can help “ensure that these systems do not undermine workers’ rights or their safety.”<sup>5</sup> The OSTP is considering a wide range of impacts on workers, including their “physical and mental health; privacy; dignity, and autonomy; and ability to exercise workplace rights.”<sup>6</sup>

We appreciate the opportunity to contribute to OSTP’s inquiry. Knowing Machines is an interdisciplinary research project tracing the histories, practices, and politics of how automated systems are trained to interpret the world from vast, nebulous datasets. Our research targets the assumptions underlying emerging machine-learning technologies with the hope that greater transparency will encourage meaningful interventions.<sup>7</sup> We are a team of lawyers, computer scientists, science and technology studies (STS) professors, artists, and data scientists who have

---

<sup>1</sup> Legal Research Fellow, The Knowing Machines Research Project; Supervising Attorney, NYU’s Technology Law & Policy Clinic, and Fellow, Engelberg Center on Innovation Law & Policy, NYU School of Law.

<sup>2</sup> Lead Principal Investigator, The Knowing Machines Research Project; Research Professor of Communication and STS, USC Annenberg School for Communication and Journalism; Senior Principal Researcher, Microsoft Research Lab (NYC).

<sup>3</sup> Co-Principal Investigator, The Knowing Machines Research Project; Professor of Clinical Law, Director of NYU’s Technology Law & Policy Clinic, and Co-Director of the Engelberg Center on Innovation Law & Policy, NYU School of Law.

<sup>4</sup> 88 Fed Reg. 27,932, available at <https://www.federalregister.gov/documents/2023/05/03/2023-09353/request-for-information-automated-worker-surveillance-and-management>.

<sup>5</sup> *Id.* at 27,934.

<sup>6</sup> *Id.*

<sup>7</sup> For more information, see <https://knowingmachines.org>.

published extensively on the techniques and harms of automated surveillance technologies, including in the workplace—whether that be the factory floor, warehouse, office, or the home.<sup>8</sup>

Knowing Machines urges OSTP to translate workers’ expectations of privacy in their data into guidance for employers on when and what types of data they can collect. As worker data fuels automated surveillance technologies by serving as training data for machine-learning models, we encourage OSTP to set a high bar for employers who exploit worker data to inform employment decision and undermine workers’ autonomy. Specifically, we propose OSTP collaborate with other federal agencies to set baseline protections over worker data that align with the limits on health data for healthcare providers and on consumer financial data for financial institutions respectively. At a minimum, we hope OSTP will adopt clear policies protecting worker data relating to union organizing communications and activities.

## I. Automated Worker Surveillance and Management Systems Depend on Massive Amounts of Worker Data

The pandemic and its aftermath have intensified existing rifts over worker autonomy and control in the U.S.<sup>9</sup> Especially as young adults enter a workforce shaped by decades-long wage stagnation, anemic unionization, and regular waves of mass layoffs, they are proving immune to the promises of “workism”—the belief that “work is not only necessary to economic production, but also the centerpiece of one’s identity and life’s purpose.”<sup>10</sup> Attention-grabbing buzzwords like “the Great Resignation”, “quiet quitting”, and the “anti-work movement” attempt to capture a

---

<sup>8</sup> See, e.g., KATE CRAWFORD, ATLAS OF AI: POWER, POLITICS, AND THE PLANETARY COSTS OF ARTIFICIAL INTELLIGENCE 53–87 (2021) [hereinafter, ATLAS OF AI]; Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL. L. REV. 101 (2017), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2746211](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211) [hereinafter *Limitless Worker Surveillance*]. See also Edward B. Kang, *Ground Truth Tracings (GTT): On the Epistemic Limits of Machine Learning*, 10 BIG DATA & Soc’y (2023) (problematizing promises of individualized “employee fit” assessments from a generalized voice biometric analytics product), <https://journals.sagepub.com/doi/epub/10.1177/20539517221146122>; Knowing Machines Rsch. Grp., Comment on Federal Trade Commission Advanced Notice of Proposed Rulemaking on Commercial Surveillance (Dec. 1, 2022) (surveying facial emotion recognition technologies deployed on job-seekers and workers), <https://www.regulations.gov/comment/FTC-2022-0053-1142>.

<sup>9</sup> See *Limitless Worker Surveillance*, *supra* note 8, at 111–13 (describing the changing nature of work in the U.S., including pre-pandemic increases in remote workers and freelance workers).

<sup>10</sup> Derek Thompson, *Working Is Making Americans Miserable*, ATLANTIC (Feb. 24, 2019), <https://www.theatlantic.com/ideas/archive/2019/02/religion-workism-making-americans-miserable/583441/>. See also Terry Nguyen, *Gen Z Does Not Dream of Labor*, VOX (Apr. 22, 2022), <https://www.vox.com/the-highlight/22977663/gen-z-antiwork-capitalism>; Kim Kelly, *Gen Z’s Not Lazy—They’re Just Refusing To Put Up with the Toxic Work Culture that Boomers Created*, BUS. INSIDER (Nov. 3, 2022), <https://www.businessinsider.com/how-gen-z-is-changing-work-most-pro-labor-generation-2022-11>.

broader sense of turmoil in our relationship to work, boundaries, and living a meaningful life both in and beyond our jobs.<sup>11</sup>

Yet workism persists, with around 40% of workers seeing their jobs as central to their overall identities regardless of gender, race, ethnicity, or age.<sup>12</sup> While certain groups of workers—educated young men, high-earners, and recovering workaholics—are spending less time working than pre-pandemic,<sup>13</sup> employers continue to project their “productivity paranoia” onto workers of all stripes.<sup>14</sup> This has led to a sharp increase in surveillance technologies permeating the average workday. Searches for employee monitoring software increased by 75% in March 2020 compared with the 2019 monthly average, and now around 80% of employers use monitoring software to track employee performance and online activity.<sup>15</sup>

Today, technology is a critical factor in both what we do for work and how we do it. But while employers have been rapidly adopting new methods of AI-driven automated worker surveillance,<sup>16</sup> this phenomenon is a continuation of much older labor practices established in the late nineteenth and early twentieth centuries.<sup>17</sup> As one of us has previously noted, “[w]e are witnessing new refrains on an old theme.”<sup>18</sup> The atomized, tedious work of early factories

---

<sup>11</sup> See Rani Molla, *Quiet Hiring and the Endless Quest To Coin Terms About Work*, Vox (Jan. 12, 2023), <https://www.vox.com/recode/23548422/quiet-quitting-hiring-great-resignation-words-about-work>.

<sup>12</sup> PEW RSCH. CTR., HOW AMERICANS VIEW THEIR JOBS (2023), <https://www.pewresearch.org/social-trends/2023/03/30/how-americans-view-their-jobs/#how-workers-see-their-job>.

<sup>13</sup> Rich Miller, *Americans Are Working Less than They Did Before the Pandemic*, BLOOMBERG (Apr. 5, 2023), <https://www.bloomberg.com/news/articles/2023-04-05/americans-emulate-europe-and-work-less-posing-problem-for-fed>.

<sup>14</sup> *Hybrid Work Is Just Work. Are We Doing It Wrong?*, MICROSOFT (Sept. 22, 2022), <https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work-is-just-work>.

<sup>15</sup> Goh Chiew Tong, *Employee Surveillance Is on the Rise—and That Could Backfire on Employees*, CNBC (Apr. 23, 2023), <https://www.cnbc.com/2023/04/24/employee-surveillance-is-on-the-rise-that-could-backfire-on-employers.html>.

<sup>16</sup> In this Response, we focus on machine learning-based technologies of worker surveillance. We use the term “AI”, aware of its misleading anthropomorphism, to refer to technical systems that rely on machine learning models trained on datasets to extract patterns and use those patterns to predict outcomes in new contexts. See generally Sarah Ciston, *A Critical Field Guide for Working with Machine Learning Datasets* (2023), <https://knowingmachines.org/critical-field-guide>.

<sup>17</sup> See ATLAS OF AI, *supra* note 8, at 59 (“[T]he encroachment of AI into the workplace should properly be understood as a return to older practices of industrial labor exploitation that were well established in the 1890s and the early twentieth century.”); Saima Akhtar, *Employers’ New Tools To Surveil and Monitor Workers Are Historically Rooted*, WASH. POST (May 6, 2021), <https://www.washingtonpost.com/outlook/2021/05/06/employers-new-tools-surveil-monitor-workers-are-historically-rooted/> (“The history of worker surveillance shows that today’s cutting-edge time-tracking technologies are just new iterations of an old industrial technique—only now, these technologies are more discreet and pervasive.”). For a robust historical analysis of worker surveillance in the U.S., see IFEOMA AJUNWA, *THE QUANTIFIED WORKER: LAW AND TECHNOLOGY IN THE MODERN WORKPLACE* 179–87 (2023).

<sup>18</sup> ATLAS OF AI, *supra* note 8, at 29.

required managers to maintain efficient and disciplined workers.<sup>19</sup> This necessitated new systems of observation and control for managers that drew from earlier systems, including the 1780s’ inspection house that placed all of a factory’s workers within constant sight of their supervisors, and the central role of overseers for slave owners in the plantation colonies of the Americas.<sup>20</sup> This historic oversight role has been “primarily deputized to surveillance technologies” today.<sup>21</sup> But what these technologies enable is a more granular and invasive degree of worker surveillance than historical human managers could ever dream of.<sup>22</sup>

There are several types of automated worker surveillance.<sup>23</sup> Much of it is deployed to placate the employer that workers are really working. This includes activity monitoring, or surveilling how workers spend their time through tools that “track[ ] idle time, record[] keystrokes, or even periodically screenshot[] an employee’s computer.”<sup>24</sup> But there are also several types of surveillance that go beyond monitoring productivity to uncover workers’ personal behaviors and characteristics. So-called “bossware” programs that monitor and collect data from workers’ emails, telephones, and online activities can be used to gauge productivity, but that data can also reveal personal behaviors and characteristics with no connection to one’s work.<sup>25</sup> Other examples include location tracking, video camera surveillance, measuring workers’ use of different applications on digital devices, and even biometric surveillance tools that use facial recognition to ensure that workers remain in front of their computer screens during business hours.<sup>26</sup> Behavioral surveillance tools not only measure productivity and compliance with company policies, but some also attempt to predict when workers might be likely to quit.<sup>27</sup> And tools like emotion recognition analysis are used to gauge a job candidate’s “fit” with the

---

<sup>19</sup> *See id.* at 60–61.

<sup>20</sup> *Id.* at 61–63.

<sup>21</sup> *Id.* at 62.

<sup>22</sup> Akhtar, *supra* note 17 (“Although the surveillance and punishment of ‘wasted time’ on the factory floor has remained fairly consistent over the past century, the way workers’ time gets tracked and recorded has become more invasive due to advancements in technology.”).

<sup>23</sup> A full survey is outside of the scope of this Response but can be found in various publications. *See, e.g.*, AJUNWA, *supra* note 17, at 187–92 (2023) (providing an overview of modern worker surveillance); *Limitless Worker Surveillance*, *supra* note 8, at 108–113 (gathering similar examples).

<sup>24</sup> AJUNWA, *supra* note 17, at 189.

<sup>25</sup> *See Limitless Worker Surveillance*, *supra* note 8, at 111 fig.1 (showing connections between various forms of surveillance and productivity, behavioral, and personal characteristic analyses); Zoë Corbyn, ‘Bossware Is Coming for Almost Every Worker’: The Software You Might Not Realize Is Watching You, *GUARDIAN* (Apr. 27, 2022), <https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic>.

<sup>26</sup> *See* AJUNWA, *supra* note 17, at 190–91.

<sup>27</sup> *Id.* at 191.

prospective employer, based on pseudoscientific conclusions about the ways we express emotions through facial gestures alone.<sup>28</sup> Sometimes, data collected from costumers—like their traffic patterns and other interactions with products and employees—lead to indirect worker surveillance, informing employers how many workers to schedule and where.<sup>29</sup>

These technologies inform the field of “people analytics” built on the vast digital data generated mostly passively as workers perform their daily activities.<sup>30</sup> Its central premise is that as much data must be collected as possible, so that these data can provide accurate insights into persistent managerial questions, including who to hire or promote, who is likely to leave, who has been working collaboratively despite working remotely, and whether workers feel fulfilled professionally.<sup>31</sup> The algorithms that interpret these data are increasingly used to inform employment decisions, whether or not workers are aware of the surveillance.<sup>32</sup>

People analytics beget an intimately quantified modern worker.<sup>33</sup> Whereas Taylorist theories of management focused on mastering a single task along the assembly line and maximizing production efficiency, people analytics has shifted focus onto the individual worker as a cite of self-mastery to save the employer time and money.<sup>34</sup> Surveillance technologies allow employers to be omnipresent in each of their workers’ lives without physically being anywhere near them, enabling uninterrupted monitoring of a person’s communications, movements, and activities even outside of work.<sup>35</sup> Employers have converted their workers into “captive audiences for data extraction,” using these technologies to indiscriminately capture and transfer worker data that is

---

<sup>28</sup> See Knowing Machines Rsch. Grp., Comment on Federal Trade Commission Advanced Notice of Proposed Rulemaking on Commercial Surveillance (Dec. 1, 2022) (surveying facial emotion recognition technologies deployed on job-seekers and workers), <https://www.regulations.gov/comment/FTC-2022-0053-1142>.

<sup>29</sup> AJUNWA, *supra* note 17, at 174.

<sup>30</sup> See Jeffrey T. Polzer, *The Rise of People Analytics and the Future of Organizational Research*, 42 ORGANIZATIONAL BEHAV. 1 (2023), [https://www.hbs.edu/ris/Publication%20Files/1-s2.0-S0191308523000011-main\\_0230d385-13af-4a01-9b68-c6b07be05ce2.pdf](https://www.hbs.edu/ris/Publication%20Files/1-s2.0-S0191308523000011-main_0230d385-13af-4a01-9b68-c6b07be05ce2.pdf).

<sup>31</sup> *Id.* at 1.

<sup>32</sup> *Id.* at 3 (“Workers are being quantified as never before as the ongoing digital revolution converts every action and interaction into a trail of data. These data can be fed into algorithm, which can then produce predictions, categorizations, and suggestions to change behavior.”). See also Alex Christian, *The Employee Surveillance that Fuels Worker Distrust*, BBC (June 27, 2022), <https://www.bbc.com/worklife/article/20220621-the-employee-surveillance-that-fuels-worker-distrust> (“Often, this [bossware] technology runs undetected, meaning workers can be unaware that their boss is effectively spying on them.”).

<sup>33</sup> See generally AJUNWA, *supra* note 17.

<sup>34</sup> *Limitless Worker Surveillance*, *supra* note 8, at 137.

<sup>35</sup> *Id.* at 138; see also AJUNWA, *supra* note 17, at 175 (“Surveillance technologies are what has enabled management to become less visible, yet more powerful.”).

often personal and sensitive.<sup>36</sup> For our colleague and worker surveillance expert Ifeoma Ajunwa, this data is “captured capital” as it “is siphoned from workers both knowingly and unknowingly as part of the employment bargain.”<sup>37</sup> Workers have no uniform privacy protections to this data,<sup>38</sup> and they largely lack any bargaining power over how employers exploit their data.<sup>39</sup>

There is a direct link between the exploitation of worker data and automated worker surveillance. Put simply, “[d]ata obtained through employee surveillance fuels AI.”<sup>40</sup> As worker data becomes more legible and sortable into distinct categories, it can be used to train machine-learning models that undergird AI technologies used to interpret worker behavior. This creates a dangerous cycle: workers use technologies that produce data, that data is compiled into vast datasets, those datasets are used to train models, those models influence algorithms to find certain associations in the data, and then those algorithms power automated surveillance tools used by employers to decide whether workers are being sufficiently productive, loyal, and compliant. Pairing the “voracious maw of data collection” with the “inexplicability of decisions made” from automated systems leads to workers feeling “trapped in a matrix of computer-controlled reality from which there is no escape.”<sup>41</sup>

There is growing concern about the misuse of data to train machine-learning models powering automated surveillance technologies, and worker data should be no exception.<sup>42</sup> In its consideration of automated worker surveillance systems, OSTP must be mindful of the enclosure of worker data that enables the development of these systems in the first place. The lack of clear privacy protections for worker data provides OSTP a unique opportunity to guide employers on when and what types of worker data they can collect, store, use, and sell. OSTP must act now to

---

<sup>36</sup> AJUNWA, *supra* note 17, at 178.

<sup>37</sup> *Id.* at 177.

<sup>38</sup> *Limitless Worker Surveillance*, *supra* note 8, at 113–28 (analyzing extant legal protections and their weaknesses).

<sup>39</sup> See ATLAS OF AI, *supra* note 8, at 58 (“The terms [of AI in the workplace] are based on a significant power asymmetry—is there ever a choice not to collaborate with algorithmic systems? When a company introduces a new AI platform, workers are rarely allowed to opt out.”); Kate Crawford, *Amazon’s Union Vote Could Be a Harbinger for the Future of Work*, WASH. POST (Apr. 10, 2021) (“Artificial intelligence systems are increasingly used to track, assess, and rank workers—often without their knowledge. This, in turn, acts as a force multiplier for the asymmetries of power between bosses and employees.”); Pauline T. Kim & Matthew T. Bodie, *Artificial Intelligence and the Challenges of Workplace Discrimination and Privacy*, 35 ABA J. LABOR & EMP. L. 289, 292 (2021), [https://www.americanbar.org/content/dam/aba/publications/aba\\_journal\\_of\\_labor\\_employment\\_law/v35/no-2/artificial-intelligence.pdf](https://www.americanbar.org/content/dam/aba/publications/aba_journal_of_labor_employment_law/v35/no-2/artificial-intelligence.pdf) (“Employees report a feeling of powerlessness when AI is given significant power over their jobs, as they lose the ability to interact with their ‘supervisor’ in a meaningful way.”).

<sup>40</sup> Kim & Bodie, *supra* note 39, at 301.

<sup>41</sup> *Id.* at 292.

<sup>42</sup> See, e.g., Kenny Peng, Arunesh Mathur & Arvind Narayan, *Mitigating Dataset Harms Requires Stewardship: Lessons from 1000 Papers*, 35th Conf. Neural Info. Processing Sys. (2021), <https://arxiv.org/pdf/2108.02922.pdf>.

counterbalance employers' insatiable thirst for more comprehensive and invasive worker data to fuel people analytics solutions, bringing autonomy over worker data explicitly into the conversation.

## II. OSTP Should Adopt Baseline Worker Data Privacy Guidance to Deter Unchecked Worker Surveillance by Employers

In its Blueprint for an AI Bill of Rights, OSTP recognized that individuals and their communities “should be free from unchecked surveillance; surveillance technologies should be subject to heightened oversight.”<sup>43</sup> Responding to Question 5. of the RFI, Knowing Machines encourages OSTP to develop guidance for employers who currently deploy automated worker surveillance systems or are considering doing so.<sup>44</sup> We are mindful that often specific statutes and regulations governing security, access, and notice and consent regimes “provide insufficient guidance for decisions about the reuse and repurposing of information when companies can manipulate huge amounts of data” collected through worker surveillance.<sup>45</sup> Instead, we agree that “broader principles have to be developed that can guide privacy decisions consistently in a variety of contexts,” and those broader principles should draw from workers' own expectations about their data “as a touchstone for developing [employers'] privacy practices, including the [employer's] definition of privacy.”<sup>46</sup> Beyond simply punishing bad behavior, federal agencies beginning with OSTP must encourage employer responsibility for protecting worker privacy.<sup>47</sup>

Because automated worker surveillance technologies require vast amounts of worker data for training purposes, employers are currently incentivized to collect worker data with abandon. OSTP should consider adopting guidance that proposes internal guardrails for employers over when and what types of worker data they are able to collect and process. To this end, we suggest OSTP help disincentive limitless worker surveillance by encouraging employers to treat worker

---

<sup>43</sup> Available at <https://www.whitehouse.gov/ostp/ai-bill-of-rights/data-privacy-2/>.

<sup>44</sup> In particular, Knowing Machines responds to 5.c., which asks “What policies or actions should Federal agencies consider to protect workers' rights and wellbeing as automated worker surveillance and management systems are developed and deployed, including through regulations, enforcement, contracting, and grantmaking?” 88 Fed Reg. at 27936.

<sup>45</sup> KENNETH A. BAMBERGER AND DEIRDRE K. MULLIGAN, *PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE* 62 (2015).

<sup>46</sup> *Id.* at 64, 65.

<sup>47</sup> *See id.* at 246.

data with the same level of care that healthcare providers treat health data<sup>48</sup> and financial institutions treat consumer financial data.<sup>49</sup> This guidance should be informed first and foremost by workers' own expectations of privacy over their communications, locations, behaviors, and other forms of personal data, especially where employers cannot show that these data and work performance are connected or such connections are attenuated at best.<sup>50</sup>

Furthermore, we encourage OSTP to explore numerous worker data protections that will impact the viability of automated surveillance technologies driven by AI today. First, OSTP should work with other agencies to develop data privacy requirements in vendor agreements for automated surveillance products, including strict data minimization procedures and use limitation requirements to ensure that only the necessary amount of data is collected for a specific employment use (ideally limited to human resources and diversity initiatives), and data collected in one context is not later applied in employment decisions in other contexts. For companies that collect worker data into databases that could be used to train automated technologies, OSTP can incentive greater clarity around database access and licensing by requiring employers to appoint dataset stewards who can decide and document how datasets may be used, derived from, and distributed outside of the employer.<sup>51</sup>

Additionally, OSTP can work with organized and organizing workers fighting back against automated worker surveillance to protect them from employer interference and retaliation. In line with recent decision by the National Labor Relations Board against Amazon's anti-union surveillance efforts, OSTP can adopt clear policies prohibiting the collection of worker data

---

<sup>48</sup> See Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936; INSTITUTE OF MEDICINE (US) COMMITTEE ON HEALTH RESEARCH AND THE PRIVACY OF HEALTH INFORMATION: THE HIPPA PRIVACY RULE (Sharyl J. Nass et al. eds., 2009).

<sup>49</sup> See Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6081–6089, 6821–6827 (1999); *Financial Privacy*, FED. TRADE COMM'N, <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/financial-privacy> (last visited June 15, 2023).

<sup>50</sup> See AJUNWA, *supra* note 17, at 202 (discussing how, when state law does not specifically prohibit worker surveillance, courts weigh an employer's need to conduct surveillance against the employee's reasonable expectation of privacy); Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS U. L.J. 21, 49 (2018), <https://scholarship.law.slu.edu/lj/vol63/iss1/4/> (“[W]hile a reasonable expectation of privacy is well defined for Fourth Amendment cases, it is not as defined within the employment context, and some scholars have argued that workplaces operate as ‘private governments’ with employers exercising near dictatorial power over what privacy rights may be granted to workers.”).

<sup>51</sup> See Peng, Mathur & Narayan, *supra* note 42, at 9–10 (describing how dataset creators should best steward datasets to minimize downstream misuses of the underlying data).



related to organizing and union participation.<sup>52</sup> By protecting workers from the weaponization of their data to thwart organizing efforts, OSTP will enable workers to collectively bargain with their employers about the specific, context-dependent limitations they seek over their own workplace surveillance and their employers' access to their personal data.<sup>53</sup>

### III. Conclusion

Knowing Machines supports OSTP's critical inquiry into the massive reach of automated worker surveillance technologies and their negative impacts on workers' lives. OSTP should develop guidance on baseline privacy protections that mediate the inherent power differential between employers and workers over control of their data. We encourage OSTP to emphasize the centrality of worker data to automated surveillance technologies powered by AI, as worker data informs the training of models that then influence algorithmic decision-making in opaque and unjust ways. If OSTP has any further questions, please reach out to Legal Research Fellow Melodi Dincer at [melodi.dincer@law.nyu.edu](mailto:melodi.dincer@law.nyu.edu) or Co-Principal Investigator Jason Schultz at [jason.schultz@exchange.law.nyu.edu](mailto:jason.schultz@exchange.law.nyu.edu).

Respectfully Submitted,



---

Melodi Dincer  
Legal Research Fellow  
Knowing Machines Research Project

---

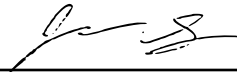
<sup>52</sup> See, e.g., Memorandum from Nat'l Lab. Relations Bd. General Counsel Jennifer A. Abruzzo to All Regional Officers, Officers-in-Charge, and Resident Officers on Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights (Oct. 31, 2022), <https://www.nlr.gov/news-outreach/news-story/nlr-general-counsel-issues-memo-on-unlawful-electronic-surveillance-and>; Press Release, Nat'l Lab. Relations Bd., NLRB Region-29 Wins Federal Court Order Requiring Amazon to Cease and Desist from Firing Employees for Protected Activities (Nov. 28, 2022), <https://www.nlr.gov/news-outreach/news-story/nlr-region-29-wins-federal-court-order-requiring-amazon-to-cease-and-desist-from-firing-employees-for-protected-activities>; Robert Iafolla, *Amazon Broke Labor Law in Anti-Union Push, NLRB Judge Rules (2)*, BLOOMBERG L. (Jan. 31, 2023), <https://news.bloomberglaw.com/daily-labor-report/amazon-broke-labor-law-in-anti-union-push-nlr-judge-rules>.

<sup>53</sup> See *Hearing from the American People: How Are Automated Tools Being Used To Surveil, Monitor, and Manage Workers?*, WHITE HOUSE OFFICE SCI. & TECH. POL'Y (May 1, 2023), <https://www.whitehouse.gov/ostp/news-updates/2023/05/01/hearing-from-the-american-people-how-are-automated-tools-being-used-to-surveil-monitor-and-manage-workers/> ("Monitoring conversations can deter workers from exercising their rights to organize and collectively bargain with their employers.").



---

Kate Crawford  
Lead Principal Investigator  
Knowing Machines Research Project



---

Jason Schultz  
Co-Principal Investigator  
Knowing Machines Research Project