Notes

Restoring Reasonable Expectations to Privacy at Work in the Face of Modern Electronic Monitoring Practices

RAFI BORTNICK[†]

This Note argues that stronger legal protections are necessary in California to protect workers' dignitary interests in the workplace in the face of prevalent electronic monitoring. In particular, those protections should be grounded in a respect for a worker's personhood rather than property rights relating to worker data collected by employers. In California, workers have some limited privacy and autonomy protections found in common law, the state constitution, and various statutes. Caselaw and legislative enactments have recognized the value of protecting personhood. The passage of the California Privacy Rights Act in 2020 marked a shift toward privacy protections grounded in data as property. This Note critiques the ability of that law to protect workers' dignitary interests. Moving past the critique, this Note offers suggestions for improving California work standards under the law today, in addition to proposing legislation to strengthen protections for workers in the future based on personhood rather than property interests.

[†] J.D. Candidate, Class of 2024, University of California College of the Law, San Francisco, Work Law Concentration. I would like to thank Professor John True for his guidance developing the topic for this Note and throughout the writing process. Also, thanks to Professors Reuel Schiller, Beth Ross, Veena Dubal, Mai Linh Spencer, and Miye Goishi at UC Law SF, and to Mike Gaitley at Legal Aid at Work, for their support and encouragement in my exploration of the complex legal landscape governing work in California.

TABLE OF CONTENTS

INTRODUCTION

In a video titled "[I] quit my $350k job as a lawyer," Cece Xie details her reasons for leaving her big law job in favor of a career as a social media influencer.[1] Her reasons include hour tracking requirements, disrespect from clients, and the inability to make change through the firm bureaucracy.[2] In sum, she was unhappy with the lack of autonomy and dignity she had at work. As the economy transitioned from manufacturing to largely service-based, the reputation, or "brand" of the firm became paramount, and employee identity became more and more enmeshed in the identity of the firm, and the firm's identity in that of its workers.[3] Employers developed a business interest in a worker's off-the-job conduct. Finally, in today's internet economy, the right to one's personality in some cases has become the right to profit from one's personality; for some, this is the ideal outcome for workers. However, for most workers, "influencing" is neither an option nor a desire.[4] "[I]f everyone's going to be an influencer, then who are they influencing?"[5] The vast majority of individuals have no meaningful opportunity to profit from use of the data property that is their "personal brand." Under a framework that treats personality as property, the right to privacy becomes very expensive for those who cannot or do not want to profit from their individuality.

In the workplace, employers explicitly limit the ways and extent to which individuals express their personal identities through policies and codes of conduct. Doing so is necessary to the effective functioning of any organization.[6] Employers have legitimate interests in the collection, use, and, in some circumstances, disclosure of data to control the workplace and protect their assets, manage liabilities, and create value for stakeholders. Employers may limit workers' individuality implicitly through the monitoring of worker activity, and the provision of incentives and disincentives for behaviors that

1. Amy Odell, *How Corporate America (Mis)manages Slash Influencers*, FAST CO. (Mar. 13, 2022), https://www.fastcompany.com/90730756/hr-social-media-policies.

2. Cece Xie, *I Quit My $350k Job as a Lawyer.*, YOUTUBE (Feb. 23, 2022), https://www.youtube.com/watch?v=1sq0bQN3Qec.

3. Matthew T. Bodie, *The Law of Employee Data: Privacy, Property, Governance*, 97 IND. L.J. 707, 736 n.193 (2022). Throughout this Note, I generally refer to "workers" rather than "employees" because many workers who are classified by employers as independent contractors—regardless of whether that classification is valid—face the same or greater exposure to electronic monitoring as do those classified as employees. Where the law or specific practices of employers refer to employees, I use that term.

4. Darian Woods, Wailin Wong, Corey Bridges, Janet W. Lee & Kate Concannon, *The Economics of the Influencer Industry*, NPR: THE INDICATOR FROM PLANET MONEY, at 4:55 (Apr. 25, 2023, 5:00 PM EST), https://www.npr.org/2023/04/17/1170524077/the-economics-of-the-influencer-industry.

5. Adrian Ma, Darian Woods, Corey Bridges & Kate Concannon, *The Dark Side of the Influencer Industry*, NPR: THE INDICATOR FROM PLANET MONEY, at 3:15 (Apr. 27, 2023, 4:17 PM EST), https://www.npr.org/2023/04/17/1170524093/the-dark-side-of-the-influencer-industry ("When your lifestyle is your brand, the line between work and life get blurred.").

6. Bodie, *supra* note 3, at 747.

drive performance metrics drawn from the data collected. Employer incursions into workers' private lives fall into three main categories: (1) the collection of information; (2) the use of information collected; and (3) the disclosure of information collected to third parties.[7] Even where monitoring is hidden from workers, the data collected will still likely drive decisions that affect the workers' behavior, in addition to implicating other privacy concerns.

Workers also have legitimate interests in both privacy and autonomy.[8] Most workers highly value their privacy at work.[9] Under California law, privacy protections mostly take the form of regulating expectations about the use of physical and virtual spaces and the disposition of specified types of personal information.[10] This creates a tension in the modern workplace where workers subject to the legitimate control of the hiring entity generate extensive amounts of data that also reflect their identities as individuals with individual interests. New software-as-a-service ("SaaS") products consolidate employers' workplace monitoring capabilities.[11] SaaS products increasingly offer insights based on artificial intelligence (AI) analysis of the vast swaths of data that previously might have gathered dust on a hard drive or in the cloud without a company devoting considerable resources to sifting through them.[12]

While it is hard to assess the nature of all these changes in real time, it is clear that much of what is changing is enabled by technological advancements.[13]

---

7. Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1181–82 (2005).

8. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654 (Cal. 1994).

9. Emily Belton, *78% of Employers Engage in Remote Work Surveillance, ExpressVPN Survey Finds*, EXPRESSVPN (Mar. 11, 2023), https://www.expressvpn.com/blog/expressvpn-survey-surveillance-on-the-remote-workforce (finding that of surveyed workers, 48% would be willing to take a pay cut in exchange for freedom from surveillance, 25% of workers by as much as by 25% of pay, 54% said they would be likely to quit if surveillance was instituted (though there are no numbers on actual quit rates), and 43% felt monitoring was a violation of trust). *But see Harris Poll Shows How to Gain Employee Support for Monitoring Programs and Avoid Privacy Invasions*, DTEX SYS. (June 27, 2018), https://www.dtexsystems.com/blog/harris-poll-gaining-employee-support-for-monitoring-programs (finding that 71% of respondents said they would not take a job if they were subject to monitoring without prior notice, but when given notice, 64% said employers have a right to monitor work or personal devices *for security purposes* (emphasis added)). Note that the Harris poll was conducted before COVID-19 related changes to work conditions and the broad exposure of the forms and extent of workplace monitoring.

10. *See* Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1072 (Cal. 2009) (discussing extensively the reasonable expectation standard for privacy claims under the state constitution and common law). *See also, e.g.*, CAL. PENAL CODE § 632(c) (West 2017) (protections against eavesdropping exclude communications the parties reasonably expect to be overheard); CAL. LAB. CODE § 435 (West 1999) (bright-line rule against audio and videotaping in locker rooms).

11. *See, e.g.*, *Using AI and Machine Learning for Monitoring Employees*, CLEVERCONTROL (Nov. 30, 2023), https://clevercontrol.com/using-ai-for-monitoring-employees.

12. *Id.*

13. MARK MURO, SIFAN LIU, JACOB WHITON & SIDDHARTH KULKARNI, BROOKINGS METRO. POL'Y PROGRAM, DIGITALIZATION AND THE AMERICAN WORKFORCE 6–7 (2017), https://www.brookings.edu/wp-content/uploads/2017/11/mpp_2017nov15_digitalization_full_report.pdf.

The vast majority of jobs today are performed to some extent with the aid of a computing device.[14] Wireless bandwidth and mobile computing improvements have allowed jobs to be performed remotely that previously would have been impossible or detrimental to detach from the employer's worksite.[15] Over the last decade, mobile technology has significantly advanced.[16] For example, improvements and reduction in size of cameras, microphones, and a host of other physical sensors allow tracking and collection of data for everything from the acceleration and deceleration of a truck on the highway to the movement of a worker's eyes across a screen.[17]

Norms have also changed, shown in stark relief during the height of the COVID-19 pandemic. At the same time, expectations about privacy have diminished as workers, in their off-the-clock capacity as consumers, have integrated new forms of technology into their personal lives. These technologies include new social media platforms and wearable devices like smart watches. Workers, consumers, have grown accustomed to hyper-targeted advertising.[18] Monitoring of workers, as agents of an employer, to some extent, has always been fundamental to the relationship. An employer's right to control the work performed would be meaningless without some sense of what workers are doing. Obscuring management decisions in data raises risks of discrimination when metrics fail to "measure the person for the job,"[19] but this is only one problematic aspect of treating workers as the data they generate. Invasive electronic monitoring presents serious threats to the physical and psychological wellbeing of workers.

According to the American Psychological Association, workers subject to electronic monitoring are nearly twice as likely as workers free from monitoring to report issues with stress at work (60%) and to experience negative impacts of the work environment on their mental health (45%).[20] A 2022 meta-analysis of job satisfaction and stress of employees subject to electronic monitoring found that workers "perceive reduced job satisfaction and increased stress when

14. *Id.* at 7.

15. *See* Jacob Lorinc, *Meet Freshii's New 'Virtual Cashier' — Who Works From Nicaragua for $3.75 an Hour*, TORONTO STAR (Apr. 26, 2022), https://www.thestar.com/business/2022/04/26/meet-the-freshii-virtual-cashier-who-works-from-nicaragua-for-375-an-hour.html.

16. *See Drastic Falls in Cost Are Powering Another Computer Revolution*, ECONOMIST (Sept. 12, 2019), https://www.economist.com/technology-quarterly/2019/09/12/drastic-falls-in-cost-are-powering-another-computer-revolution; *see also* Memorandum from Jennifer A. Abruzzo, Gen. Couns., NLRB, to All Regional Directors, Officers-in-Charge, and Resident Officers 1 (Oct. 31, 2022), https://apps.nlrb.gov/link/document.aspx/09031d45838de7e0.

17. ECONOMIST, *supra* note 16.

18. Ian Bogost, *Welcome to the Age of Privacy Nihilism*, ATLANTIC (Aug. 23, 2018), https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198.

19. Griggs v. Duke Power Co., 401 U.S. 424, 436 (1971).

20. *Workers Appreciate and Seek Mental Health Support in the Workplace*, AM. PSYCH. ASS'N, https://www.apa.org/pubs/reports/work-well-being/2022-mental-health-support (last visited Apr. 28, 2024).

monitored. On an organizational level, it is likely that there is no gain in employees' performance but increased deviant behavior."[21] An earlier study found that workers "who had their performance electronically monitored perceived their working conditions as more stressful, and reported higher levels of job boredom, psychological tension, anxiety, depression, anger, health complaints and fatigue."[22] In addition, "[w]orkplaces with higher levels of ESAM [Electronic Surveillance and Algorithmic Management] often experience an increase in the number of physical workplace injuries."[23] Several times throughout the State's history, Californians have declared that the prolific collection of personal information, by both government agencies and businesses, presents an unacceptable risk to individual privacy interests. Judges, regulators, the legislature, and citizens have sought to enact stronger protections for privacy. But the law today does not protect against these diffuse harms to worker physical and mental health caused by monitoring.[24]

Part I of this Note explores the modern workplace in greater detail, including the types of information generated by workers in the ordinary course of business, the competing interests of workers and employers in data collection and use, and the development of electronic monitoring systems. It describes trends and explores examples of products emblematic of the monitoring technology available in the market. Part II explores the history of legal protections for the privacy of workers in California, which may provide some protections for workers against excessive workplace monitoring. It then turns to the law today, with particular focus on the California Privacy Rights Act adopted by ballot measure in 2020 that went into effect January 1, 2023. Part II also discusses current gaps in the law and their connection to the harms of the modern workplace electronic monitoring practices laid out in Part I. Finally, while employers also should consider the impact of monitoring on worker health, Part

21. Rudolf Siegel, Cornelius J. König & Veronika Lazar, *The Impact of Electronic Monitoring on Employees' Job Satisfaction, Stress, Performance, and Counterproductive Work Behavior: A Meta-Analysis*, 8 COMPUT. HUM. BEH. REPS., Dec. 2022, at 1, 10; *see also* Martha Ockenfels-Martinez, *Blog: Workplace Surveillance Harms Essential Workers*, OTHERING & BELONGING INST. (Jan. 21, 2021), https://belonging.berkeley.edu/blog-workplace-surveillance-harms-essential-workers.

22. M. J. Smith, P. Carayon, K. J. Sanders, S.-Y. Lim, & D. LeGrande, *Employee Stress and Health Complaints in Jobs With and Without Electronic Performance Monitoring*, 23 APPLIED ERGONOMICS 17, 17 (1992).

23. Reed Shaw, Anna Rodriguez & Matt Scherer, *Definitions & Background: ESAM Poses a Risk to Workers' Physical Health*, *in* ELEC. SURVEILLANCE & ALGORITHMIC MGMT. 01-1, 01-5 (Apr. 3, 2023), https://cdt.org/wp-content/uploads/2023/04/Complete-Electronic-Workplace-Surveillance-OSHA-NIOSH-memo-package.pdf.

24. IFEOMA AJUNWA, THE QUANTIFIED WORKER: LAW AND TECHNOLOGY IN THE MODERN WORKPLACE 178 (2023) ("As it stands, there is no bright-line law that delineates what data employers may extract from workers and how such data may be used."); Lewis Maltby, *Employment Privacy: Is There Anything Left?*, A.B.A. (May 1, 2013), https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/2013_vol_39/may_2013_n2_privacy/employment_privacy.

III offers suggestions for actions that judges, workers, the legislature, and enforcement agencies can take to ensure workers' rights are better protected in this age of nearly limitless electronic monitoring in the workplace.

I. THE MODERN WORKPLACE

The New York Times recently published the groundbreaking work, *The Rise of the Worker Productivity Score*.[25] The online version of the piece contains a number of metrics viewable to each reader: time spent on the site, amount of the article scrolled through, number of links clicked, keystrokes, idle time, and active time percentage.[26] At the end of the piece, the site presents a score and offers suggestions for improvement of the reader's experience, which may include "reading comprehension" if the reader scrolled too quickly.[27] Scrolling to the bottom of the site too slowly produces pop-up warnings about the pace of reading.[28] To be clear, the New York Times did not actually *retain* these metrics for each reader in a database.[29] But the article details the many ways in which employers do engage in this type monitoring, recording, and tracking. Jobs subject to such practices are not limited to warehouse workers on an assembly line.[30] They include "[a]rchitects, academic administrators, doctors [and radiologists], nursing home workers [and hospice chaplains], and lawyers."[31]

Companies also now have the technology to digitalize, offshore, and outsource more jobs and more discrete functions of jobs than at any time in the past. This includes the "manufacturization" of service jobs that previously would not have been computer-based.[32] Many services traditionally performed by one individual can now be broken into discrete functions to be performed repetitively and in series by a team, akin to an assembly line, or even dispersed individuals.[33]

---

25. Jodi Kantor & Arya Sundaram, *The Rise of the Worker Productivity Score*, N.Y. TIMES (Aug. 14, 2022), https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html; *see also* Michael Barbaro & Jodi Kantor, *The Rise of Workplace Surveillance*, N.Y. TIMES: THE DAILY (Aug. 24, 2022), https://www.nytimes.com/2022/08/24/podcasts/the-daily/workplace-surveillance-productivity-tracking.html (discussing monitoring software used in the workplace); Drew Harwell, *Managers Turn to Surveillance Software, Always-on Webcams to Ensure Employees Are (Really) Working from Home*, WASH. POST (Apr. 30, 2020, 10:24 AM EDT), https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance (discussing the use of surveillance software on work from home employees).

26. Kantor & Sundaram, *supra* note 25.

27. *Id.*

28. *Id.*

29. Kate Dwyer, *Don't Worry, We're Not Actually Monitoring Your Productivity*, N.Y. TIMES (Aug. 19, 2022), https://www.nytimes.com/2022/08/19/insider/productivity-tracker.html.

30. *Id.*

31. Kantor & Sundaram, *supra* note 25.

32. Amanda Aronczyk, Kenny Malone, Emma Peaslee & Keith Romer, *Would You Like a Side of Offshoring With That?*, NPR: PLANET MONEY (Sept. 30, 2022, 5:22 PM EST), https://www.npr.org/2022/09/30/1126167551/would-you-like-a-side-of-offshoring-with-that.

33. *See* AJUNWA, *supra* note 24, at 36–37.

Freshii, a Canadian fast-food chain, recently began employing cashiers who interact with customers by appearing via a video screen and who work from home in countries in Central and South America.[34] This type of arrangement would not have been possible even a few years ago due to constraints on internet bandwidth that limited video conferencing capabilities.[35]

While much has been said about the shift to remote work, for the purposes of assessing workers subjection to electronic monitoring, the "on-site" versus "off-site" distinction matters a lot less than computer and internet connectivity on the job.[36] Workers using a computing device can be monitored through their interaction with that device, or in some cases through their mere proximity to the device.[37] Data can then be extracted, aggregated, and analyzed—the workers are evaluated across a number of metrics beyond simply counting their output.[38] Quantifying how many workers perform their jobs through a device, however, is difficult because of the variety of devices used in different work contexts.[39] One survey in 2021 found that "81% of employees are using one or more employer-provided device."[40]

Looking at the percentage of workers who are able to perform their jobs remotely can be a helpful proxy to set a minimum threshold of workers who use devices, although measurements vary.[41] A United States Department of Labor survey in the summer of 2021 found that nearly 40 percent of companies had employees teleworking at least some of the time.[42] In the spring of 2022, 58 percent of Americans reported being able to work from home at least some of the time.[43] In 2023 and into 2024, companies have reported struggling to bring

34. Lorinc, *supra* note 15.

35. Aronczyk et al., *supra* note 32.

36. Kantor & Sundaram, *supra* note 25 ("[I]n-person workplaces have embraced the tools as well. Tommy Weir, whose company, Enaible, provides group productivity scores to Fortune 500 companies, aims to eventually use individual scores to calibrate pay. 'The real question,' he said, 'is which companies are going to use it and when, and which companies are going to become irrelevant?'"); *see also* AJUNWA, *supra* note 24, at 187.

37. AJUNWA, *supra* note 24, at 174.

38. *Id.*

39. James E. Bessen, *Information Technology and Learning On-the-Job* 12–13 (B.U. Sch. of L., L. & Econ. Working Paper No. 16-47, 2016), http://www.ssrn.com/abstract=2867134.

40. Belton, *supra* note 9.

41. Emma Goldberg, *Do We Know How Many People Are Working from Home?*, N.Y. TIMES (Apr. 2, 2023), https://www.nytimes.com/2023/03/30/business/economy/remote-work-measure-surveys.html.

42. Bureau of Lab. Stats., U.S. DEP'T OF LAB., *Telework, Hiring, and Vacancies – 2022 Data from the Business Response Survey*, https://www.bls.gov/news.release/pdf/brs1.pdf.

43. André Dua, Kweilin Ellingrud, Phil Kirschner, Adrian Kwok, Ryan Luby, Rob Palter & Sarah Pemberton, *Americans Are Embracing Flexible Work – And They Want More of It*, MCKINSEY & CO. (June 23, 2022), https://www.mckinsey.com/industries/real-estate/our-insights/americans-are-embracing-flexible-work-and-they-want-more-of-it.

workers back to offices.[44] Electronic monitoring of remote, inherently computer-based workers is very likely the norm now.[45]

A. COMPETING INTERESTS IN THE SUBJECTS OF WORKPLACE ELECTRONIC MONITORING PRACTICES

Workplace monitoring implicates interests of both workers and employers. Workers have an interest in autonomy and an interest in privacy. Employers, on the other hand, have an interest in control over the disposition of their assets for efficiency, productivity, and risk reduction. In the workplace, privacy exists in the interstices of the relationship between principal and agent.[46] Worker privacy tests the limits of what needs to be shared to enable that relationship to function as contracted. For example, to reduce the risk of theft, Amazon searches its warehouse workers before they are permitted to leave its facilities.[47] In California, Governor Newsom appointed the Future of Work Commission in 2019 to make recommendations about (among other things) the impact of technology on work.[48] The commission noted that:

---

44. *See* Greg Iacurci, *Return to Office is 'Dead,' Stanford Economist Says. Here's Why*, CNBC (Dec. 4, 2023, 3:59 AM EST), https://www.cnbc.com/2023/11/30/return-to-office-is-dead-stanford-economist-says-heres-why.html; Robin Madell, *8 Workplace Trends to Eye for 2024*, US NEWS & WORLD REP. (Nov. 27, 2023, 9:31 AM), https://www.usnews.com/careers/articles/8-workplace-trends-to-eye-for-2024.

45. Belton, *supra* note 9; *see also* Zoë Corbyn, *'Bossware is Coming for Almost Every Worker': The Software You Might Not Realize is Watching You*, GUARDIAN (Apr. 27, 2022, 4:30 AM EDT), https://www.theguardian.com/technology/2022/apr/27/remote-work-software-home-surveillance-computer-monitoring-pandemic. The founder of Basecamp has pushed back against the use of monitoring that he believes amounts to surveillance, refusing to allow those products to integrate with Basecamp software. Corbyn, *supra.* This seems to be an exception to the general trend of integrated SaaS systems. Danielle Abril, *Your Boss Can Monitor Your Activities Without Special Software*, WASH. POST (Oct. 9, 2022, 7:00 AM EDT), https://www.washingtonpost.com/technology/2022/10/07/work-app-surveillance; Harwell, *supra* note 25 (noting that Zoom briefly employed an attention tracking feature, but removed it after public backlash); *Non-Tech Businesses Are Beginning to Use Artificial Intelligence at Scale*, ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/non-tech-businesses-are-beginning-to-use-artificial-intelligence-at-scale; David Leonhardt, *You're Being Watched*, N.Y. TIMES (Aug. 15, 2022), https://www.nytimes.com/2022/08/15/briefing/workers-tracking-productivity-employers.html.

46. AJUNWA, *supra* note 24, at 177.

47. *See* Integrity Staffing Sols., Inc. v. Busk, 574 U.S. 27, 35 (2014). The Court upheld the Amazon practice of making employees wait as long as twenty-five minutes after their shifts ended to pass through security screenings to prevent theft. *Id.* at 30.

48. *Future of Work Commission*, LAB. & WORKFORCE DEV. AGENCY (2021), https://www.labor.ca.gov/labor-and-workforce-development-agency/fowc.

> Technology enables companies to monitor worker behavior across industries and workplaces, including productivity in warehouses, customer service centers, and retail stores. Increasingly, white-collar workplaces employ technology to monitor and collect data on employees, and can even track movements through an office building, regulating speed of work and bathroom use as an employee's smartphone connects to different Wi-Fi routers.[49]

The rest of this section briefly assesses the employer interests that lead to use of electronic workplace monitoring technologies. It then turns to the workers' interests in privacy and autonomy implicated when these technologies are used.

1. *Employer Interests in Monitoring Workplaces and Workers*

Employers cite their top two reasons for using electronic monitoring as increasing productivity[50] and improving risk management.[51] The quintessential productivity-related fear of employers is "time theft," which happens when workers clock-in or log hours but do not actually work during that time. In one recent case in Canada, a worker was ordered to repay wages to her employer after the organization's time-tracking software logs conflicted with her manually entered timesheet.[52] Screen captures showed she engaged in what the software designated as personal use of her work computer during times she purported to be working.[53] While the Society for Human Resources Management (SHRM) advises employers this type of recovery is much more difficult in the United States,[54] employers may nevertheless be tempted to electronically monitor workers in order to deter time theft or to quickly discover and correct this

49. FUTURE OF WORK COMM'N, LAB. & WORKFORCE DEV. AGENCY, FUTURE OF WORK IN CALIFORNIA: A NEW SOCIAL COMPACT FOR WORK AND WORKERS 29 (2021), https://www.labor.ca.gov/wp-content/uploads/sites/338/2021/02/ca-future-of-work-report.pdf.

50. At least at a macroeconomic level, productivity has risen faster than real wages for several decades—well before more recent increases in the scope of electronic monitoring at many workplaces. *The Productivity–Pay Gap*, ECON. POL'Y INST. (Oct. 2022), https://www.epi.org/productivity-pay-gap. This measure of productivity does not factor in time spent waiting for work in the on-demand context. In conversation with U.S. Bureau of Labor Statistics National Compensation Survey staff. *See also infra* note 126 and accompanying text (discussing how electronic monitoring enables the productivity–pay gap in the "gig" economy).

51. AJUNWA, *supra* note 24, at 186–87.

52. Megan Cerullo, *Spy Software Found a Worker Wasn't Working as Much as She Said. Now She Must Repay Her Wages.*, CBS NEWS: MONEYWATCH (Jan. 13, 2023, 2:54 PM EST), https://www.cbsnews.com/news/remote-worker-ordered-to-repay-employer-after-tracking-software-shows-time-theft.

53. *Id.*

54. Allen Smith, *Can US Employers Recover Damages from Former Employees for 'Time Theft'?*, SHRM (Feb. 1, 2023), https://www.shrm.org/topics-tools/employment-law-compliance/can-us-employers-recover-damages-former-employees-time-theft.

behavior.[55] Software providers cite time theft deterrence as part of marketing their programs to employers.

Employers also have reason to be concerned about worker misuse of electronic systems. Companies faced new liability for employee misuse of email and mismanagement of data following the passage of the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the Sarbanes-Oxley Act of 2002 ("SOX").[56] Many began hiring "human-resource forensics" specialists to increase electronic monitoring of employees.[57] This seemed to portend a shift from targeted investigations to regular electronic monitoring of all employees. "[W]hile companies still use cameras and phone taps to track down the bad eggs and sometimes even send detectives into the office to poke around for evidence after hours, most scrutiny focuses on computers, the weapon of choice for corporate wrongdoers."[58] Employers may also investigate workers before making employment decisions. Discussing constitutional privacy rights in the workplace, John Barker notes:

> Employers often want private information about an employee that is neither required nor directly job-related. The higher a position is in a company's hierarchy, the more personal commitment the company may require. If a company is contemplating a promotion to a front-line management position, or a promotion from an hourly job to a salaried job, it may have a special interest in an employee's capacity for commitment.[59]

These inquiries are a form of due diligence. Employers may even owe a fiduciary duty to debtors and shareholders to conduct these inquiries. In some ways, at least in a non-unionized workplace, the employer also represents the interests of an individual worker's coworkers and customers in a safe, stable workplace. This means employers *should* exercise some supervision and control of workers for the common benefit. In some instances, California requires employers to share a worker's personal information with state regulators.[60] Whether for the employer's own analysis or in response to legal requirements, "[t]he upshot is this: employment now means handing over even more of our individual selves, in the form of data, in service to a communal enterprise."[61]

---

55. Tom Spiggle, *Can Employers Monitor Employees Who Work From Home Due to the Coronavirus?*, FORBES (May 21, 2020, 9:48 AM EDT), https://www.forbes.com/sites/tomspiggle/2020/05/21/can-employers-monitor-employees-who-work-from-home-due-to-the-coronavirus.

56. Marci Alboher Nusbaum, *Executive Life; New Kind of Snooping Arrives at the Office*, N.Y. TIMES (July 13, 2003), https://www.nytimes.com/2003/07/13/business/executive-life-new-kind-of-snooping-arrives-at-the-office.html.

57. *Id.*

58. *Id.*

59. John C. Barker, *Constitutional Privacy Rights in the Private Workplace, Under the Federal and California Constitutions*, 19 HASTINGS CONST. L. Q. 1107, 1148 (1992).

60. CAL. LAB. CODE § 1174(a)–(c) (West 2012).

61. Bodie, *supra* note 3, at 717.

2. *Worker Dignitary Interests in Privacy and Autonomy*

Electronic monitoring poses a substantially greater risk to workers than the physical presence of a supervisor in terms of both scale and intrusiveness.[62] One of the problems is that workers, even when given notice, may ignore banal monitoring that occurs behind the scenes on work devices. They may not even care about the particular metrics the employer is tracking when considered individually, but the aggregation of data about individual workers may be incredibly invasive.[63] When aware of monitoring, workers may experience psychological stress from being watched and measured. Further, workers may feel pressure to change behaviors, for example, by working at a faster pace than they otherwise would.[64] Worker awareness of monitoring may changes the workers' behavior in an effort to meet the goals of the employer regarding the specific monitored activity.[65] However, academics and judges may disagree on the extent of this "observer effect."[66] When unaware of monitoring—either in form or scope—workers may divulge personal information they would otherwise intend to keep private *from their employers*. Because the employment relationship is based in agency and contract, workers have diminished autonomy rights within the context of the relationship.[67] In addition, employer policies

62. *See* AJUNWA, *supra* note 24, at 80, 149.

63. *See generally id.*

64. *See id.* at 53, 176 ("Surveillance technology that is laser focused on the productivity of individual workers serves to recreate much the same 'speed-up' as the Taylorist workplaces . . ." where managers measured workers with a stopwatch.).

65. Veena Dubal, *On Algorithmic Wage Discrimination*, 123 COLUM. L. REV. 1929, 1939–41 (2023). In this article, Dubal examines the way platform companies mine data from workers to allow them to engage in what she terms "algorithmic wage discrimination." *Id.* at 1934. Dubal discusses how this happens in two different ways, "(1) wages based on productivity analysis alone [which we see most clearly] (in the employment context), and (2) wages based on productivity, supply, demand, and other personalized data used to minimize labor costs," whether that happens through gamification or psychological tricks. *Id.* at 1934 n.15. As a "highly personalized and variable form of compensation," algorithmic wage discrimination was adopted by on-demand, labor platform companies to:

> solve a particular problem that accompanies the (mis)classification . . . . Since drivers are not treated as employees of the firm and the primary legal indicum of employment status is control . . . , firms often do not directly order workers as to where they must go and when they must go there . . . . Instead, the firms use data extracted from workers' labor and fed into automated tools to incentivize temporal and spatial movement.

Id. at 1946.

Dubal would solve the specific problem of this form of data harvesting and use with an outright ban on the practice of setting wages in this way. *Id.* at 1940.

66. *See* Hilda Bastian, *The Hawthorne Effect: An Old Scientists' Tale Lingering "in the Gunsmoke of Academic Snipers*,*"* SCI. AM. (July 26, 2013), https://blogs.scientificamerican.com/absolutely-maybe/the-hawthorne-effect-an-old-scientistse28099-tale-lingering-e2809cin-the-gunsmoke-of-academic-sniperse2809d/; Will Kenton, *Hawthorne Effect Definition: How It Works and Is It Real*, INVESTOPEDIA (June 15, 2022), https://www.investopedia.com/terms/h/hawthorne-effect.asp.

67. *See* discussion *infra* Part II.A.1.

disclosing monitoring reduce or negate a worker's expectation to privacy within the work context.[68]

While dignitary interests play a strong role in worker dissatisfaction with electronic monitoring practices, pecuniary interests, if not as salient in discussions of intrusive software as misuse of personal information, are likely more pressing for the majority of workers.[69] Much of the issue with productivity monitoring boils down to both employers' and workers' interest in fair and accurate pay for work performed. "[T]he most urgent complaint, spanning industries and incomes, is that the working world's new clocks are just wrong: inept at capturing offline activity, unreliable at assessing hard-to-quantify tasks and prone to undermining the work itself."[70] But workers also still have an interest in privacy that extends beyond the material implications of inaccurate information collected about them. Privacy is about dignity. As Samuel Warren and Judge Louis Brandeis discuss in their seminal work, *The Right to Privacy*:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[71]

Judge Brandeis and Warren wrote these words over a century ago, but they hold no less true today. At that time, a major concern was the growing use of photographs by newspapers.[72] Arguing that greater protections for privacy were needed in the face of this then-emerging technology and its application in business, this foundational article traced the development of common law principles of rights to "life" and "property," which grew to encompass interests

---

68. *See* discussion *infra* Part II.A.1.

69. *See* AJUNWA, *supra* note 24, at 52–53 (discussing workers in the 1910s feeling cheated by Frederick Taylor's prototypical time tracking system of "scientific management" (Taylorism) that was intended to "get the most out of [each worker]."). Estimates vary, and there are many ways to measure financial precarity, but as an example, an early 2023 report from Lending Club found that more than half of Americans live paycheck to paycheck, including many earning over $100,000 a year. *See* Press Release, LendingClub, 60% of Americans Now Living Paycheck to Paycheck, Down from 64% a Month Ago (Feb. 28, 2023), https://ir.lendingclub.com/news/news-details/2023/60-of-Americans-Now-Living-Paycheck-to-Paycheck-Down-from-64-a-Month-Ago/default.aspx.

70. Kantor & Sundaram, *supra* note 25; *see also* Drew Harwell, *Contract Lawyers Face a Growing Invasion of Surveillance Programs that Monitor Their Work*, WASH. POST (Nov. 11, 2021, 8:00 AM EST), https://www.washingtonpost.com/technology/2021/11/11/lawyer-facial-recognition-monitoring ("Contract attorneys . . . have become some of America's first test subjects for this enhanced monitoring, and many are reporting frustrating results, saying the glitchy systems make them feel like a disposable cog with little workday privacy.").

71. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

72. *Id.* at 195.

beyond the everyday meaning of those terms.[73] "[T]he right to life has come to mean the right to enjoy life—*the right to be let alone*; the right to liberty secures the exercise of extensive civil privileges; and the term 'property' has grown to comprise every form of possession—intangible, as well as tangible."[74] The common law further developed to recognize "[t]houghts, emotions, and sensations" as within the scope of protectable interests included in a right to privacy.[75] Crucially, the individual interest at stake in personal privacy matters is not the protection of a material property interest—as intruded on in cases of libel, slander, and copyright infringement—but rather individuals' right to be secure in their persons, to determine for themselves what they communicate to others about themselves.[76] More succinctly, the interest is "the right to one's personality," not just to a personal brand that can be marketed.[77]

3. *Property Interests in Data Generated by and About Workers*

Property interests in worker data complicate the discussion. "The key marker of employee data is that it derives from a particular person—an individual employee—but it is not confined to 'personal' information."[78] So when a worker is performing tasks "in the scope of employment," the data collected by the employer in the process may result in "property rights that were once assigned to the individual becom[ing] group property—owned by the employing enterprise."[79] This includes workers' personal data collected by the employer. The sum of this personal data and the inferences that may be drawn from it in some sense comprises the worker's identity. The common law right to publicity allows individuals to sue when someone else uses their identity without their consent.[80] "The right of publicity has been characterized both as a right to privacy as well as a personal IP [intellectual property] right—something akin to trademark for people."[81]

Where employers draw inferences from worker data to create profiles, workers may have a cause of action for violations of their rights to publicity, but this is largely untested in workplace related litigation.[82] Further, employment contracts may grant any property rights in employee data to the employer, and job applicants would likely have difficulty negotiating over assignment of these

73. *Id.* at 193.
74. *Id.* (emphasis added).
75. *Id.* at 195.
76. *Id.* at 198–200.
77. *Id.* at 207.
78. Bodie, *supra* note 3, at 712.
79. *Id.* at 725–26.
80. *Id.* at 728.
81. Bodie, *supra* note 3, at 728.
82. *Id.* at 729.

rights. For example, covenants not to compete, nondisclosure agreements, and the standardized assignment of intellectual property rights to work products can preclude workers from discussing their "working identity" with future prospective employers.[83]

Grounding privacy protections in property interests leaves both employers and workers worse off in the workplace context.[84] It puts a value on data that might otherwise be considered priceless, incentivizing the collection of data through monitoring. It also creates a zero-sum game for the disposition of that data. Because employers have a legitimate interest in the collection of data related to their businesses, workers' interests in prevention of unnecessary monitoring would be inadequately protected by a tort after data collection has occurred.

The addition of the California Consumer Privacy Act (CCPA) to the California employment privacy landscape creates the hybrid approach of blending privacy and property rights to protect workers, as argued for by employment law scholar Matt Bodie,[85] but only to a very limited extent. Most of the value of worker data is in relation to the individual worker within the workplace context from which the data is derived. Putting privacy aside, workers necessarily have a greater interest in employers' decisions based on their data than in the monetary value of that data when sold to a third party. Where disputes arise, courts would be ill-equipped to make valuations of individual worker data outside of a market context—where the dispute is over the collection and use of the data within the workplace.

83. *Id.* at 738.

84. *Id.* at 748. There is a hybrid approach that would grant certain property rights to workers in data collected by employers while also relying on privacy law to shield workers from excessive data collection. *See id.* at 747–48. Assigning fiduciary duties to employers in relation to worker data would likewise be useful, but it only adds another avenue for workers to seek a remedy for the misuse of data, rather than preventing high risk collection of data in the first place. *See id.* at 748–51. Such an approach to strengthening protections for workers' interests in data, however, still requires defining the data to which workers have rights. Because of the difficulty of defining that data, legislators should rather focus on setting limits for data collection methods and uses by employers, and encourage individual and collective bargaining over the actual use of properly collected data. *See infra* Part II.B.; *see also* AJUNWA, *supra* note 24, at 177 (discussing "captured capital" in worker data: "The work of legal scholar Matthew Bodie tends to support an argument against employer exploitation of employee data without just compensation.").

85. *See also* AJUNWA, *supra* note 24, at 177.

B. MODERN ELECTRONIC MONITORING MARKS A PARADIGM SHIFT IN THE AGENCY RELATIONSHIP

> "The postal mail comes once a day, but people see hundreds or thousands of new renditions of their own private information in the same time on online."[86]

Workplace monitoring has changed significantly in recent years.[87] Monitoring is one aspect of the "war to quantify not just the output of the worker, but also the gestalt of the ideal worker."[88] In the past, a worker could reasonably expect to be subject to certain physical searches at workplaces, or to be watched by an on-site supervisor. Today, employee monitoring software has reduced the costs of collecting and analyzing vast amounts of data from workers and allows employers to make inferences about employee preferences and mental states, in some cases without the worker's knowledge or consent.[89] Through these means, as described below, employers may extract more value from an individual worker than merely from the work the individual performs as an agent of the employer. Employers now extract something of the workers as individuals.

1. *Historical Development of Monitoring Technologies*

Workplace monitoring has grown in sophistication in tandem with the technology used by workers. In some cases, employers capture data about workers incidentally; analysis blurs the lines between worker data and business transactional data.[90] Monitoring technology has been developed to meet management's desire for control over a workplace transformed by the introduction of new technology.[91] For example, the introduction of the Internet to workplaces gave workers more tools to perform job functions, but also created more potential for distraction and security risks, leading employers to seek tools to observe what workers were doing when they are using company computers.[92] This mostly took the form of searches of discreet electronic records.[93] Modern, sophisticated electronic monitoring systems go much further than their

86. Bogost, *supra* note 18.

87. *See generally* AJUNWA, *supra* note 24.

88. *Id.* at 138.

89. Mihalis Kritikos, *Workplace Monitoring in the Era of Artificial Intelligence*, EPRS (Dec. 22, 2020), https://epthinktank.eu/2020/12/22/workplace-monitoring-in-the-era-of-artificial-intelligence ("Workplace surveillance is age-old, but it has become easier and more common, as new technologies enable more varied, pervasive and widespread monitoring practices and have increased employers' ability to monitor apparently every aspect of workers' lives."); Phoebe V. Moore, *Data Subjects, Digital Surveillance, AI and the Future of Work*, PANEL FOR THE FUTURE OF SCIENCE AND TECHNOLOGY 31 (2020), https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)656305.

90. AJUNWA, *supra* note 24, at 188.

91. *Id.* at 171.

92. Mark S. Dichter & Michael S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, 5 LEGALFOCUS ON PROPERTY & GENERAL LIABILITY INSURANCE 42, 44 (2001).

93. *Id.* at 43–44.

antecedents of a few decades ago, generating real-time reports on worker behavior based on automated inferences of collected data.

In the on-demand economy, companies may be much less concerned with productivity than in a traditional workplace. As employment law scholar Veena Dubal describes:

> Instead of using data and automation technologies to increase productivity by enabling workers to work more efficiently in a shorter period (to decrease labor overhead), on-demand companies like Uber and Amazon use data extracted from labor, along with insights from behavioral science, to engineer systems in which workers are less productive (they perform the same amount of work over longer hours) and receive lower wages, thereby maintaining a large labor supply while simultaneously keeping labor overhead low.[94]

The difference between on-demand and traditional employment models may be due to the variance in the elasticity of the labor pools for those sectors. If it takes significantly more resources to recruit and train employees than it does on-demand independent contractors, employers have a greater incentive to extract more output from individual employees. Regardless, these examples emphasize an employer's interest in managing labor costs by manipulating the productive capacity of its workforce. Electronic monitoring systems, at least in part, enable this manipulation in either the on-demand or traditional employment context.

As another example, consider how electronic monitoring and data collection enables employer control in another type of work arrangement that in some ways bridges the gap between the "gig" economy and longer-term employment relationships: the highly-controlled franchise. A series of court cases in the 1970s enabled corporations to exert more control over franchisees without running afoul of antitrust laws.[95] In 7-Eleven stores, this meant the franchisor was able to install cameras and monitor live-feeds in the franchisees' stores, and even install thermostats that could only be operated by the corporation.[96] The franchisor also had the power to change what items franchisors were able to sell in real time based on analysis of sales data transmitted back to the franchisor.[97] Without these electronic tools, it would be impossible for a franchisor to exercise such a high level of control across thousands of stores without a massive investment in supervisory labor to monitor and control the work performed by franchisees.

---

94. Dubal, *supra* note 65, at 1965.

95. Sam Harnett, *How Franchising Paved the Way for the Gig Economy*, KQED (Mar. 18, 2021), https://www.kqed.org/news/11862641/how-franchising-paved-the-way-for-the-gig-economy.

96. *Id.*

97. *Id.*

But to effectively replace physical monitoring with automated electronic monitoring, employers in any context first need the ability to quantify and track work activities and compare metrics with a benchmark as well as other data relevant to the analysis of worker performance. One of the most important technological advancements to meet this end was the development of the relational database in the 1970s.[98] A relational database is essentially a system that records data in tables linked logically by identifiers.[99] The relational database gave organizations the ability to link individual performance metrics with productivity and sales metrics. For example, one recommendation for call centers in 1999 was to link scores from live monitoring of employee performance to sales data.[100] "The same type of analysis can be performed with employee analysis software to incorporate an employee development strategy measured in 'hard-measures' (such as profitability and production) instead of 'soft-metrics' (such as employee satisfaction)."[101]

"Almost every important enterprise-software program of the [1980s]—most of which ordinary people never thought about or saw—was built atop the idea of a relational database."[102] In an effort to expand sales opportunities, Target used a relational database system in 2012 to link customer sales data with other data purchased from data brokers to identify customers going through major life events in order to capture a potential change in their purchasing habits (a rare occurrence).[103] In a test case, Target statisticians assigned customers a "pregnancy prediction" score by analyzing their shopping patterns and sent them coupons for pregnancy and baby-related products based on the customer's expected due date.[104] This practice is known as "targeted" or "behavioral" advertising, and is common practice today.[105] After receiving negative reactions, Target decided to mix the coupons in with others for random products to make it seem less like they were inferring pregnancy and parental status.[106] However, they continued to make those inferences.[107]

98. *What Is A Relational Database (RDBMS)?*, GOOGLE CLOUD, https://cloud.google.com/learn/what-is-a-relational-database (last visited Apr. 15, 2024); Bogost, *supra* note 86.

99. *What Is A Relational Database (RDBMS)?*, *supra* note 98; Bogost, *supra* note 86.

100. Abby Miller, *Track Employee Development with a Relational Database*, DMNEWS (May 7, 1999), https://www.dmnews.com/track-employee-development-with-a-relational-database.

101. *Id.*

102. Bogost, *supra* note 86.

103. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

104. *Id.* (discussing how this campaign, in at least one case, resulted in a father learning that his high-school aged daughter was pregnant before she had told him).

105. *Factsheet: Surveillance Advertising: What Is It?*, CONSUMER FED'N AM. (Aug. 26, 2021), https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-what-is-it.

106. Duhigg, *supra* note 103.

107. *Id.*

Connected-workplace tools and devices log and transmit data, including managerial observations, customer feedback, and transactions conducted by the worker. Activities, like making a sale, clocking-in, or opening certain software, are now more easily quantifiable. Employers can also correlate transactions with other data. For example, a worker's heart rate could have been checked and logged occasionally in the past but the collection of that data would have necessitated disrupting the work being performed. Now, an unobtrusive wearable device can automatically correlate heart rate data with other employer data related to the worker and make inferences about how a worker's health affects job performance, all without disturbing the workflow.

Employers may also purchase workers' personal information from data brokers, creating challenges for workers attempting to avail themselves of privacy protections that regulate property interests in data or limit an employer's direct collection of personal information from workers. This is discussed further in Part IV.D.3, in relation to rights under the California Consumer Privacy Act. Recently, companies have begun to deploy AI to find correlations that were previously effectively hidden within larger data sets.[108] AI allows for analysis of much larger datasets than practicable or cost effective when done by direct analysis, thereby incentivizing the collection of more datapoints.

2. *Recent Technological Innovations Facilitate Invasive Monitoring*

While a lot of media focuses on the possibilities of workplace monitoring technology, practical applications of these technologies are predictable when viewed in light of the employer's interests in productivity and risk management. Most practices are also perfectly legal, and banal. Monitoring to support productivity analysis serves a legitimate business interest in profitability, as does monitoring to ensure compliance with laws and security of the workplace.[109] The unique risk presented by excessive electronic monitoring comes from the psychological stress placed on workers subjected to working under a microscope.[110] The possibility of employers drawing inferences from data that do not reflect the worker's chosen expression of their identity, and the leveraging of data to undermine and further erode workers' bargaining power to negotiate

108. *See* DANIEL KAHNEMAN, OLIVIER SIBONY & CASS R. SUNSTEIN, NOISE: A FLAW IN HUMAN JUDGEMENT 111–36, 392–95 (2021) (discussing the ability of algorithmic data analysis to produce stronger correlations from large datasets than clinical observations); *see also AI Providers Will Increasingly Compete with Management Consultancies*, ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/ai-providers-will-increasingly-compete-with-management-consultancies.

109. Request for Information; Automated Worker Surveillance and Management, 88 Fed. Reg. 27932, 27932 (May 3, 2023), https://www.federalregister.gov/documents/2023/05/03/2023-09353/request-for-information-automated-worker-surveillance-and-management.

110. Shaw, Rodriguez & Scherer, *supra* note 23, at 01-6–01-8.

over the terms and conditions of employment threaten long established public policies setting minimum standards for employment in California.[111]

Data comes from common work tools like computers, but also from more novel sources. Human Resources analytics company Humanyze puts its own technology into practice with its workers.[112] "Everyone is wearing an ID [identification] badge the size of a credit card and the depth of a book of matches. It contains a microphone that picks up whether they are talking to one another; Bluetooth and infrared sensors to monitor where they are; and an accelerometer to record when they move."[113] Wearable devices like these personal ID badges are becoming more commonplace. "Amazon has patented a wristband that tracks the hand movements of warehouse workers and uses vibrations to nudge them into being more efficient."[114] Biometric data may be collected from employees through a variety of devices. In workplaces "the most common uses of [biometric identifiers (which include retina or iris scans, fingerprints, voiceprints, or scans of hand or face geometry)] are for timekeeping purposes . . . (to avoid time theft), or for access to secure buildings or areas . . . ."[115] "Cogito, a startup, has designed AI-enhanced software that listens to customer-service calls and assigns an 'empathy score' based on how compassionate agents are and how fast and how capably they settle complaints."[116] All of these applications of these technologies are generally legal throughout the United States.[117]

In 2016, The Wall Street Journal reported on ways in which employers had begun using personal data collected from employees in combination with information purchased from data brokers to make inferences about the likelihood of employee health events, including whether a worker was likely to become pregnant in the near future.[118] While the purpose of these analyses were to help both workers and employers reduce the cost of healthcare, the aggregation of workers' personal data in combination with work-related data collected on-the-

111. Request for Information; Automated Worker Surveillance and Management, 88 Fed. Reg. at 27932.

112. *There Will Be Little Privacy in the Workplace of the Future*, ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/there-will-be-little-privacy-in-the-workplace-of-the-future.

113. *Id.*

114. *The Workplace of the Future*, ECONOMIST (Mar. 28, 2018), https://www.economist.com/leaders/2018/03/28/the-workplace-of-the-future.

115. *Illinois Supreme Court Rejects Workers' Compensation Act Preemption of Biometric Information Privacy Act Claims*, BURKE, WARREN, MACKAY & SERRITELLA (Feb. 3, 2022), https://www.burkelaw.com/alert-Burke-Warren-News-Alert-020322.

116. *The Workplace of the Future*, *supra* note 114.

117. *See infra* Part II.

118. Rachel Emma Silverman, *Bosses Tap Outside Firms to Predict Which Workers Might Get Sick*, WALL ST. J. (Feb. 17, 2016, 7:58 PM ET), http://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940.

job by the employer creates the risk that inferences could bleed into employment decisions.[119]

When the COVID-19 pandemic hit, there was a rush among some organizations to implement technological solutions for contact tracing and health monitoring. One form of this was a health screening form workers were asked to fill out before entering a workspace, asking questions about fevers, coughs, and close contacts in the past twenty-four hours or more. Other workplaces instituted temperature monitoring cameras, wearable "proximity detection sensors" to enable contact tracing, and the "BioButton," a small device attached to the skin that aims to detect virus symptoms.[120] "They range from standard thermometer guns to more sophisticated social-distancing and heat-detection cameras, some of which are paired with facial-recognition software that security officials can use to track and identify the suspected unwell."[121] In 2020, a university in Michigan "had initially planned to require athletes and dorm residents to wear the BioButton. But the university reversed course . . . after nearly 2,500 students and staff members signed a petition objecting to the policy. The tracker [became] optional for students."[122]

Law offices appear to have implemented electronic monitoring at similar rates as in other industries, and for the same reasons of productivity and data security.[123] Legal-industry journalist Jordan Rothman recounts how a contract attorney was terminated because "[t]he software could tell when keyboards went idle and if the contract attorney was not as productive at reviewing documents as others."[124]

Professor Veena Dubal, who has written extensively on the precarious work of the "gig economy,"[125] examines one modern application of extensive data collected from workers in the "gig economy" context, what she terms

119. *Id.*

120. Natasha Singer, *The Hot New Covid Tech Is Wearable and Constantly Tracks You*, N. Y. TIMES (Nov. 15, 2020), https://www.nytimes.com/2020/11/15/technology/virus-wearable-tracker-privacy.html.

121. Drew Harwell, *Companies' Use of Thermal Cameras to Monitor the Health of Workers and Customers Worries Civil Libertarians*, WASH. POST (Apr. 28, 2020, 10:55 AM EDT), https://www.washingtonpost.com/technology/2020/04/27/companies-use-thermal-cameras-speed-return-work-sparks-worries-about-civil-liberties.

122. Singer, *supra* note 120.

123. Jordan Rothman, *Workplace Monitoring Is Commonplace in the Legal Industry*, ABOVE L. (Aug. 31, 2022, 5:17 PM), https://abovethelaw.com/2022/08/workplace-monitoring-is-commonplace-in-the-legal-industry.

124. *Id.*

125. Veena Dubal, *Wage Slave or Entrepreneur?: Contesting the Dualism of Legal Worker Identities*, 105 CALIF. L. REV. 65, 67 (2017); Veena B. Dubal, *The Drive to Precarity: A Political History of Work, Regulation, & Labor Advocacy in San Francisco's Taxi & Uber Economies*, 38 BERKELEY J. EMP. & LAB. L. 73, 76 (2017); Veena Dubal, *The New Radical Wage Code*, 15 HARV. L. & POL'Y REV. 511, 511 (2021); Veena B. Dubal, *Economic Security & the Regulation of Gig Work in California: From AB5 to Proposition 22*, 13 EUR. LABOUR L.J. 51, 60 (2022).

"algorithmic wage discrimination." The term "refer[s] to a practice in which individual workers are paid different hourly wages—calculated with ever-changing formulas using granular data on location, individual behavior, demand, supply, and other factors—for broadly similar work."[126] In addition to advances in machine learning that enable employers to implement this type of payment regime, Dubal points to the sheer scope of data collected as a prerequisite.[127] This type of data collection is beginning to be applied in workplaces in many other industries.[128] It remains to be seen whether automated, granular labor pricing will follow.

3. *Third-Party Monitoring Software Marketing Language*

Surveys of the most popular monitoring software show that the majority allow for monitoring of employee software and internet use, keystroke logging,[129] screen monitoring (including the ability to take screenshots), and email and instant message monitoring.[130] "Some of the most common [uses] are time tracking, productivity tracking, compliance with data protection laws, and IP theft prevention."[131] Companies can run many of these programs without the worker's knowledge.[132] And while audio and video recording are not the norm, those features are not hard to come by either.[133]

126. Dubal, *supra* note 65, at 1933–34. As an example of algorithmic wage discrimination in practice, Dubal writes that "[t]he company's machine learning technologies may even predict the amount of time a specific driver is willing to wait for a fare." *Id.* at 1950. This should be considered a violation of the worker's privacy interest because it intrudes on the worker's ability to negotiate fairly with the company.

127. *Id.* at 1930.

128. *Employee Surveillance Report*, SURFSHARK, https://surfshark.com/employee-surveillance (last visited Apr. 17, 2024) ("Some [remote computer monitoring systems] use algorithms to balance your productivity against your wages to literally figure out whether you're worth the money you're paid.").

129. *See What Is Keystroke Logging and Keyloggers?*, KASPERSKY, https://usa.kaspersky.com/resource-center/definitions/keylogger (last visited Apr. 17, 2024) ("Keystrokes are how you 'speak' to your computers. Each keystroke transmits a signal that tells your computer programs what you want them to do. These commands may include: length of the keypress; time of keypress; velocity of keypress; name of the key used. When logged, all this information is like listening to a private conversation." (formatting altered)).

130. *Employee Surveillance Report*, *supra* note 128; *Somebody's Watching Me: Employee Monitoring*, PRIVACYRIGHTS.ORG (June 27, 2019), https://privacyrights.org/resources/somebodys-watching-me-employee-monitoring; Bennett Cyphers & Karen Gullo, *Inside the Invasive, Secretive "Bossware" Tracking Workers*, ELEC. FRONTIER FOUND. (June 30, 2020), https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers; *see also* Neil McAllister, *The Best Employee Monitoring Software for 2024*, PCMAG (Oct. 9, 2023), https://www.pcmag.com/picks/the-best-employee-monitoring-software; Jennifer Simonson & Kelly Main, *Best Employee Monitoring Software of 2024*, FORBES ADVISOR (Mar. 21, 2024, 8:46 PM), https://www.forbes.com/advisor/business/software/best-employee-monitoring-software; Brian Stone, *The 10 Best Employee Monitoring Software Choices*, TECHREPUBLIC (Mar. 24, 2023), https://www.techrepublic.com/article/employee-monitoring-software.

131. Cyphers & Gullo, *supra* note 130.

132. *Employee Surveillance Report*, *supra* note 128.

133. *Id.* Also, it is worth noting that the recording may in some instances run afoul of wiretapping laws. *See* CAL. LAB. CODE § 435 (West 1999).

Software providers tell employers that they need to "trust but verify" and that these practices benefit workers by allowing companies to shorten meetings, or even identify non-productive times and grant workers time off during those periods.[134] Some advertise the surveillance aspects of their technology explicitly. "Work Examiner specifically advertises its product's ability to capture private passwords."[135] The most popular platforms charge around seven dollars per user per month.[136]

In 2020, "[s]everal time-tracking and employee-monitoring companies, including ActivTrak, Hubstaff, Time Doctor and Teramind, told The Washington Post they have seen their customer base and revenue soar since the pandemic pushed many companies remote."[137] The rest of this subpart briefly reviews four companies that sell popular versions of monitoring or tracking software: Hubstaff, ActivTrak, Veriato, and Samsara.[138]

Hubstaff provides one of the most popular products on the market.[139] The company bills its software as a sophisticated time tracking service that centers worker privacy.[140] Hubstaff also offers employers a webpage with advice on assessing the pros and cons of employee monitoring, as well as ethical and legal risks.[141] To show that they are not providing what they deem "spyware," Hubstaff states that workers receive notifications "when the timer starts and stops, and when screenshots are taken . . . . It's clear when Hubstaff is running

134. Patrick Thibodeau, *'Trust but Verify' May Boost Employee Productivity Monitoring*, TECHTARGET (Apr. 26, 2022), https://www.techtarget.com/searchhrsoftware/news/252516365/Trust-but-verify-may-boost-employee-productivity-monitoring.

135. Cyphers & Gullo, *supra* note 130.

136. Brian Stone, *The 10 Best Employee Monitoring Software Choices for 2023*, TECHREPUBLIC (Mar. 24, 2023), https://www.techrepublic.com/article/employee-monitoring-software; *Top 10 Employee Time Tracking Software to Use for Free or at a Rock-Bottom Price*, WORK EXAM'R, https://www.workexaminer.com/blog/top-10-employee-time-tracking-software-to-use-for-free-or-at-a-rock-bottom-price.html.

137. Harwell, *supra* note 25.

138. ActivTrak boasts 9000 customers and 550,000 users. Megan Moller, *Keeping Up with Electronic Monitoring Legislation: Transparency Is Key*, ACTIVTRAK (Apr. 14, 2022), https://www.activtrak.com/blog/electronic-monitoring-legislation-changes. Hubstaff has 95,000 business customers. *About Us*, HUBSTAFF, https://hubstaff.com/about (last visited Apr. 18, 2024). Samsara states it has "tens of thousands" of customers. *Quick Facts*, SAMSARA, https://www.samsara.com/company/about (last visited Apr. 18, 2024). Veriato, formerly SpecterSoft, does not publicly share its number of customers, however, as recently as 2016, the company—one of the pioneers in the industry—appears to have had somewhere around 35,000 customers and has likely grown significantly since that time. *SpectorSoft Changes Name to Veriato to Reflect Growing Demand for Corporate Truth*, BUSINESSWIRE (Mar. 15, 2016, 6:07 AM EDT), https://www.businesswire.com/news/home/20160315005693/en/SpectorSoft-Changes-Name-to-Veriato-to-Reflect-Growing-Demand-for-Corporate-Truth.

139. *See e.g.*, Stone, *supra* note 130.

140. *Employee Monitoring Software*, HUBSTAFF, https://hubstaff.com/features/employee_monitoring (last visited Apr. 19, 2024) ("The software tracks keyboard and mouse activity — but never to obtain sensitive data (no keystroke logging). Instead, it measures the frequency of a user's mouse and keyboard strokes . . . .").

141. *Everything You Need to Know About Employee Monitoring*, HUBSTAFF, https://hubstaff.com/employee_monitoring (last visited Apr. 19, 2024).

and when it's not."[142] The company lists recommended steps for implementing their system: obtain buy-in from workers and explain the benefits. For example, that workers will "never be underpaid again" and will "get more recognition" for their work.[143] Hubstaff also suggests having a written policy and soliciting employee feedback.[144] The company even offers an "Employee monitoring policy template."[145] The company also mentions that "[i]n the U.S., '[for] the most part, private employees have no right to privacy . . . .'"[146]

ActivTrak sells another popular option for employers.[147] Both Hubstaff and ActivTrak boast dozens of third-party software integrations, such as Google and Microsoft products, Slack, Zoom, ADP,[148] and more.[149] ActivTrak adds categorization and analysis.[150] "Data is aggregated and categorized in numerous ways: productive vs. unproductive activity, focus time vs. multitasking, email vs. meeting software vs. social media, etc."[151] ActivTrak goes further and allows customers to evaluate standardized worker productivity metrics against the entire ActivTrak customer base as a benchmark.[152] Along with benchmarking, ActivTrak touts its data security,[153] and recommends transparency,[154] but its marketing is directed more toward management's interest in productivity than workers' interests in privacy and fairness.[155] Employers purchase the software, not workers. Software providers must center employer interests. To aid

142. *Id.*

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.* Of course, many of the same concerns apply to public employees. *See Watch Out: Navigating the Legal Risks of Employee Surveillance Software*, LIEBERT CASSIDY WHITMORE (Nov. 22, 2022), https://www.lcwlegal.com/news/watch-out-navigating-the-legal-risks-of-employee-surveillance-software.

147. Stone, *supra* note 130.

148. ADP provides Human Resources Information System and Payroll software.

149. *Everything You Need to Know About Employee Monitoring*, *supra* note 141; *Get Instant Visibility into Employee Productivity and Engagement.*, ACTIVTRAK, https://www.activtrak.com (last visited Apr. 19, 2024).

150. *Get Instant Visibility into Employee Productivity Engagement*, *supra* note 149.

151. *How ActivTrak Works*, ACTIVTRAK, https://www.activtrak.com/how-it-works (last visited Apr. 19, 2024).

152. Productivity Lab, *ActivTrak Benchmarks Guide*, ACTIVTRAK (Nov. 3, 2022, 9:22AM), https://support.activtrak.com/hc/en-us/articles/4404929331995-ActivTrak-Benchmarks-Guide ("This benchmarks guide lets you easily compare your productivity, focus, and collaboration time metrics against those of our customer base and set goals accordingly. We have analyzed data from approximately 150,000 ActivTrak users and established benchmarks for the median, upper quartile (75th percentile) and lower quartile (25th percentile) for 3 metrics – Productive, Collaboration, and Focus Time.").

153. *We're Serious About Data Privacy and Security*, ACTIVTRAK, https://www.activtrak.com/security/ (last visited May 22, 2024).

154. *9 Tips to Effectively Manage a Remote Workforce with ActivTrak*, ACTIVTRAK, https://www.activtrak.com/resources/solution-briefs/9-tips-remote-work (last visited Apr. 19, 2024).

155. *Id.*

employers with compliance, ActivTrak lists state privacy laws in a table on its website.[156]

Whereas Hubstaff focuses on the benefits of its software for workers, and ActivTrak focuses on the benefits for good management, Veriato leans into employer distrust of workers, projecting risks of theft and fraud in marketing its "Vision" product to small businesses.[157] "Vision can run in stealth mode, so that no one knows it's monitoring their device."[158] Advertising states that Vision can monitor remote employees whether they are at home or travelling, claiming "when we say Vision sees everything, we mean it."[159] Advertisements presuppose workers engage in time theft.[160] "You'll quickly see who's working, and who isn't."[161] Other use cases include gathering evidence for HR or legal proceedings.[162] The more advanced offering from Veriato, "Cerebral," also touts "AI-powered [individual] behavior analysis & risk scoring."[163] In contrast, the company's blog offers advice in posts such as "How to Rebrand 'Bossware' at Your Company."[164]

Veriato suggests checking laws in the jurisdiction in which the employer operates, in addition to stating that it is legal to monitor employees without their knowledge or consent.[165] Their copy assures employer-customers that "[t]here aren't many cases, and they tend to go against the employee. Often, court opinions take the point of view that when the employees are using employers' property . . . employees' expectation of privacy is minimal."[166]

Samsara operates in a different space than the rest of the software providers on this list, focusing primarily on industrial and shipping applications.[167] Samsara makes software to monitor workers and allow employers to intervene to correct unsafe behaviors in real time.[168] These applications have clear benefits for worker and third-party safety. For example, the company offers AI assisted

156. Moller, *supra* note 138.

157. Veriato Vision, *Employee Monitoring Software for Small Businesses*, YOUTUBE (Dec. 9, 2019), https://www.youtube.com/watch?v=u9BnQ3ws0WQ.

158. *Id.*

159. *Id.*

160. *Id.*

161. *Id.*

162. *Id.*

163. *Veriato Pricing: Workforce Behavior Analytics for Every Budget*, VERIATO, https://veriato.com/pricing (last visited Apr. 19, 2024).

164. Elizabeth Harz, *How to Rebrand 'Bossware' at Your Company*, VERIATO (Aug. 8, 2022), https://veriato.com/blog/how-to-rebrand-bossware-at-your-company.

165. Veriato Team, *Is Employee Monitoring Legal?*, VERIATO (July 24, 2017), https://veriato.com/blog/is-employee-monitoring-legal.

166. *Id.*

167. SAMSARA, https://www.samsara.com (last visited Apr. 19, 2024).

168. *Id.*

dashboard and cabin cameras for truck fleets.[169] The dashboard camera faces out, away from the driver, and can provide real time alerts if the driver is too close to other vehicles on the road or can detect when the vehicle proceeds without making a complete stop at a stop sign.[170] The cabin camera faces inward to monitor the driver and can automatically send an alert if the driver is not wearing a seatbelt, looks at their phone, or even just appears to be distracted.[171] "With real-time incident detection and preventative in-cab coaching, Samsara AI Dash Cams are proven to protect drivers and lower costs."[172] Similarly, site-based cameras can automatically detect "coachable events" like workers not wearing high-visibility safety gear or having near misses (that may otherwise go unreported) and saving video of those events to a cloud based database.[173] While there may be overall cost savings to a company deploying this type of monitoring and alert system, proactive safety monitoring has potentially lifesaving benefits for workers.

Though aggregate data analysis features less prominently in Samsara's advertising, the software still collects and stores this worker data.[174] This collection presents the same risks to workers, including stress and job dissatisfaction, as software deployed in other contexts. And for all its benefits to workers, Samsara does not seem to explicitly discuss how its customers can or should protect the privacy of their workers subject to monitoring.[175] Even where monitoring presents clear benefits to worker safety, workers' interests in privacy and autonomy should be considered in the implementation of monitoring systems.

II. LAWS PROTECTING CALIFORNIA WORKERS' DIGNITARY INTERESTS AGAINST INVASIVE MONITORING

Under the California Constitution, individual privacy is a fundamental right.[176] It does not solely concern governmental intrusion, but rather focuses on an individuals' right to keep their personal life free from intrusion by others.[177]

169. *Video-Based Safety – Build a World Class Safety Program*, SAMSARA, https://www.samsara.com/products/safety (last visited Apr. 19, 2024).

170. *Id.*

171. *Id.*

172. *AI Dash Cams*, SAMSARA, https://www.samsara.com/uk/products/safety/dash-cam (last visited May 12, 2024).

173. *Video Surveillance Software: Why You Should Consider an Intelligent VMS*, SAMSARA (Aug. 6, 2021), https://www.samsara.com/guides/video-surveillance-software.

174. *See* SAMSARA, *supra* note 167.

175. *See generally id.*

176. Barker, *supra* note 59, at 1130–31.

177. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994) ("In summary, the Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities.").

In the workplace, where the "reasonable expectations" standard is predicated on the agency relationship and contracts that the worker voluntarily entered into, the right may be nullified.[178] Though an agency relationship assumes cooperation between the parties, the law generally assumes worker and management interests are adverse.[179]

In 1977, the California legislature passed the Information Practices Act, and codified its intent to strengthen the protections of the constitution in light of then-modern technological developments:

> The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:
>
> - (a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.
> - (b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.
> - (c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

That law applied to personal information collected by State agencies.[180] The legislature has repeatedly sought to address harms caused by specific uses of a worker's personal information. For example, anti-discrimination statutes like the Fair Employment and Housing Act (FEHA) serve to protect workers and job applicants against the *discriminatory use* of personal information.[181] The common law accounts for some of a worker's dignitary interests in keeping certain personal information private with the tort of invasion of privacy. The California Consumer Privacy Act passed in 2019 is the state's most recent attempt to address essentially the same risks as applied to business collection of data.[182] However, because of the ability of companies to aggregate data from

178. *See* AJUNWA, *supra* note 24, at 202.

179. *See id.* at 63–64 (discussing the adversarial division between laborers and supervisors as a foundational assumption in the law as seen in the NLRA and its amendments).

180. CAL. CIV. CODE § 1798.45 (West 2022).

181. *See* CAL. GOV'T CODE § 12940(a) (West 2023).

182. Privacy: Personal Information: Businesses, A.B. 375, 2017-2018 Sess. (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 ("(d) As the role of technology and data in the every day lives of consumers increases, there is an increase in the amount of personal information shared by consumers with businesses. California law has not kept pace with these developments and

many sources, not just from workers themselves, the opaque methods used by algorithms to draw inferences, and the reluctance of employers to reveal their data, laws like CCPA will likely prove ineffective even to deliver meaningful transparency to workers. More fundamentally, workers were an afterthought in this consumer-oriented legislation. To adequately address the harms posed by excessive electronic monitoring in the workplace, legislation specifically tailored to that issue is needed.

A. PROTECTIONS BASED ON REASONABLE EXPECTATIONS TO PRIVACY IN ONE'S PERSONHOOD

1. *Common Law and Contractual Rights to Privacy in the Workplace*

The common law in California generally protects privacy interests against four tortious actions: (1) intrusion upon seclusion; (2) appropriation of identity; (3) public disclosure of private facts; and (4) false light.[183] Under these torts, workers have a remedy when their rights have been violated, but the deterrent value of these protections is limited to an employer's knowledge of the law, expectation of private enforcement, and, in the context of electronic monitoring and use of collected data, its cost-benefit analysis of the value of that data compared with the actual damages it would have to pay to the worker. Though appropriation of identity, public disclosure of private facts, and false light torts may provide workers some remedies, the intrusion upon seclusion tort is the most applicable to workplace monitoring.[184]

Intrusion upon seclusion is available to a person who has had their "solitude or seclusion" intruded upon by another in a way that is "highly offensive to a reasonable person,"[185] meaning "the nature, manner, and scope of the intrusion are clearly unreasonable when judged against the employer's legitimate business interests or the public's interests in intruding."[186] Even where an employee has a reasonable expectation of privacy, that may not be enough to shield their personal information from examination by the employer. The law balances workers' interests and employers' rights to protect their interests based on reasonable expectations of privacy.[187] For example, when workers download

---

the personal privacy implications surrounding the collection, use, and protection of personal information. . . . (i) . . . it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information . . . .").

183. RESTATEMENT (THIRD) OF EMP. L. § 7.01, cmt. a (AM. L. INST. 2015); RESTATEMENT (SECOND) OF TORTS § 652A (AM. L. INST. 1977).

184. One hypothetical example of an emerging technological trend that could lead to Appropriation of Identity or False Light claims is AI applications that create worker profiles from collected data and write emails on behalf of workers without their consent.

185. RESTATEMENT (THIRD) OF EMP. L. § 7.01, cmt. b.

186. *Id.* § 7.06.

187. *Id.* § 7.03.

content on workplace computers where employers have provided notice that computers are monitored, they cannot expect that content to be private from their employers.[188] In general, notice and consent, whether as a best practice or a legal requirement, cannot provide workers a meaningful choice to protect their own privacy because of the economic imbalance between workers and employers.[189]

Employer privacy policies only provide protection to workers to the extent that the parties include the policy in the employment contract, as opposed to unilateral statements of policy by an employer. The California Supreme Court has held that employers' employee privacy policies cannot be imputed to employment contracts because doing so would be at odds with at-will employment.[190] In 2001, while surveying early caselaw involving employers accessing employee email, management-side legal advisors noted that "plaintiffs had no reasonable expectation of privacy in their e-mail messages because they had signed a waiver form stating that it was company policy that employees restrict their use of company-owned computer hardware and software to company business."[191]

Even where employers fail to provide notice of monitoring, without explicitly permitting workers to use company software and hardware for personal use, workers may still not have a reasonable expectation to privacy.[192] Additionally, when workers use personal accounts for business communications, they might forego a complete expectation of privacy in those non-work accounts.[193] For example, discovery in a lawsuit might implicate both personal and business messages. Likewise, privacy concerns may not preclude discovery of data collected from workers through an employer's use of

188. *Id.*

189. AJUNWA, *supra* note 24, at 162–64 (discussing notice and consent in the context of job candidates submitting to automated video interviews and finding consenting to the practice may be seen as part of the employment bargain and because of power imbalances workers may be unlikely to assert their rights for fear of losing employment opportunities).

190. Rulon-Miller v. Int'l Bus. Machs. Corp., 162 Cal. App. 3d 241, 243–44, 247–51 (1984).

191. Dichter & Burkhardt, *supra* note 92, at 45.

192. *See* RESTATEMENT (THIRD) OF EMP. L. § 7.03(b)(2) (implying a factual question of whether, in the absence of notice, an employer has treated an electronic location as private).

193. Seth Bruneel, R. Benjamin Cassady, Lionel Lavenue & Eric Magleby, *Litigation, Professional Perspective – When Personal Emails Become Discoverable*, BLOOMBERG L. (Dec. 2020), https://www.bloomberglaw.com/external/document/X250CD4C000000/litigation-professional-perspective-when-personal-emails-become ("The *Ultravision* decision cracks open the door for discovery of personal email accounts. However, employees and employers can take precautions to ensure that the door remains tightly closed and avoid having their personal matters ending up in the public record."). *But see, e.g.*, Nakanelua v. United Pub. Workers, AFSCME, Loc. 646, AFL-CIO, No. CV 20-00442 JAO-KJM, 2021 WL 6498865 (D. Haw. Nov. 5, 2021) (denying discovery and stating that "[r]esolution of this dispute turns on whether Defendants have control over these individuals' personal email accounts." Finding the employer did not have control of the email accounts, the court did not reach the issue of whether the employees' expectations of privacy in their personal emails would prevent discovery.).

electronic monitoring.[194] Employers also likely have significant latitude to share data collected from workers if it serves a legitimate business interest, especially if the employer makes no representation that it will protect the information.[195] It seems likely that only the most egregious forms of undisclosed electronic monitoring—those without a legitimate business interest—would result in liability for this tort.

In many ways, the question of where to draw the line for what constitutes a reasonable practice of worker monitoring and data collection comes down to the likely consequences of misuse and improper disclosure of personal information, as well as societal risk tolerance. Imposing fiduciary duties on employers when handling worker data would bolster common law protections.[196] Doing so would serve to limit an employers' use of data, disincentivize misuse of data, and lower the threshold for workers to bring common law tort and contract claims. But without regulating the modes and scope by which employers collect worker data, the inherent risks in excessive monitoring and data collection remain.

2. *Constitutional Rights to Privacy in the Workplace*

Generally, the Fourth Amendment of the United States Constitution protects individuals from unreasonable searches by the government.[197] The reasonableness of searches depends on the expectation of privacy and the scope of the search.[198] Because of the requirement of state action, the Fourth Amendment has a very limited application in private workplaces. The California Constitution, on the other hand, explicitly includes a right to privacy in Article I that applies to private actors:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.[199]

Early workplace right to privacy cases have focused on searches. The California Supreme Court restricted the use of polygraph testing of public

194. *See e.g.*, Williams v. Super. Ct., 398 P.3d 69, 83 (Cal. 2017); Dichter & Burkhardt, *supra* note 92, at 50 ("Similarly, discovery requests for computer information can often lead to the recovery of old e-mails, prior versions of documents, employer's motives and private assessments of an individual employee.").

195. RESTATEMENT (THIRD) OF EMP. L. § 7.05(b).

196. *See* AJUNWA, *supra* note 24, at 177–78.

197. O'Connor v. Ortega, 480 U.S. 709, 714–15 (1987).

198. *Id.* at 716–18; *cf.* City of Ontario v. Quon, 560 U.S. 746, 757 (2010) ("The case can be decided by determining that the search was reasonable even assuming Quon had a reasonable expectation of privacy.").

199. CAL. CONST. art. I, § 1; *see also* Wilkinson v. Times Mirror Corp., 215 Cal. App. 3d 1034, 1046 (1990) ("[T]he state's constitutional right to privacy protects at least to some extent against private as well as state conduct . . . .").

employees in 1986 after employees of a state agency sued to stop the practice.[200] Similar to many electronic monitoring practices,[201] polygraph examinations use sensors to quantify physical attributes of the person subject to the test.[202] Based on those measurements, the examiner makes inferences about the person's mental state in order to recommend, in this case, employment actions.[203] The court stated that "[i]f there is a quintessential zone of human privacy it is the mind. Our ability to exclude others from our mental processes is intrinsic to the human personality."[204] The court found that "[a] polygraph examination is specifically designed to overcome this privacy . . ." and that "[w]here polygraph testing is used as a preemployment screening device, 'fishing expeditions' and shockingly intrusive questions have been reported."[205]

What many workers subject to the electronic monitoring of today face is similar to an ongoing polygraph examination: roughshod recording of physical states, sometimes with the aid of devices attached to the body, in a coercive setting, where there is no ability to opt out of providing data because even a non-response is a recordable datapoint. At the time *Long Beach City Employees Association v. City of Long Beach* was decided, the California legislature, recognizing the inherent risk of abuse in this form of data collection and analysis, had already enacted a ban on the use of polygraph testing by private employers.[206] The court extended the ban to public employees based on the state constitutional right to privacy.[207]

In practice, California courts ultimately analyze the constitutional right similarly to the common law torts of invasion of privacy.[208] In *Hill v. National Collegiate Athletic Association*, the California Supreme Court reversed an injunction prohibiting the NCAA's drug testing program that involved observed urine collection.[209]

---

200. Long Beach City Emps. Ass'n v. City of Long Beach, 719 P.2d 660, 672 (Cal. 1986).

201. *See* discussion *supra* Parts I.B.2, I.B.3.

202. Mark Harris, *The Lie Generator: Inside the Black Mirror World of Polygraph Job Screenings*, WIRED (Oct. 1, 2018), https://www.wired.com/story/inside-polygraph-job-screening-black-mirror.

203. *Id.*

204. *Long Beach City Emps. Ass'n*, 719 P.2d at 663.

205. *Id.* at 663, 665 ("The intrusiveness of polygraph questions on private matters is exacerbated by three factors that make the process fundamentally different from verbal interrogation. First, '[t]he polygraph merely records general emotional arousal. It cannot distinguish anxiety or indignation from guilt.' . . . Second, an employee who is asked an embarrassing personal question may be reluctant to refuse to answer it for fear of appearing dishonest. . . . Finally, even if an employee chooses not to verbally answer a question on a personal matter, the polygraph will record his or her psychological response in any event. 'Intrusion occurs because the polygraph device continuously records the monitored physiological functions.'").

206. CAL. LAB. CODE § 432.2 (West 2022); see also discussion *infra* Part II.D.1.

207. *Long Beach City Emps. Ass'n*, 719 P.2d. at 663 ("[P]olygraph examinations inherently intrude upon the constitutionally protected zone of individual privacy.").

208. Hill v. Nat'l Collegiate Athletic Ass'n., 865 P.2d 633, 641 (Cal. 1994).

209. *Id.* at 666.

> Observation of urination and disclosure of medical information may cause embarrassment to individual athletes. The first implicates autonomy privacy—an interest in freedom from observation in performing a function recognized by social norms as private. The second implicates informational privacy—an interest in limiting disclosure of confidential information about bodily condition. But, as we have noted, the identification of these privacy interests is the beginning, not the end, of the analysis.[210]

Because the plaintiffs *voluntarily chose* to participate in the NCAA, and the "unique set of demands" of the athletic program included necessary physical observation, the students had a diminished reasonable expectation of privacy.[211]

Ultimately, the court laid out three requirements for prevailing on a claim for invasion of the constitutional right to privacy: (1) a legally recognized privacy interest;[212] (2) a reasonable expectation of privacy; and (3) a serious invasion of the privacy interest that is not outweighed by a legitimate business interest.[213] Courts must conduct a fact-heavy analysis of each claim in order to balance the worker and employer interests.

If electronic workplace monitoring is considered a search, a court's analysis of the California constitutional protection would likely include the form and scope of monitoring, company policies and employment contracts, communications between the worker and the employer, industry standards, and the nature of the use of the data collected by the employer. While singular investigations into electronic systems resemble physical searches,[214] constant, ongoing monitoring of job-related activities that generates large volumes of data may be treated differently. However, workers may not expect the data they create on the job to be private while still expecting the inferred information to be private from the employer. Today, workers' expectations of privacy may vary greatly based on their exposure to technology. Expectation may potentially also correlate with divergences along other lines, such as wealth, income, and some protected classes, meaning workers in different types of classes may enjoy different levels of protection under the law.[215]

When the right to privacy was adopted by ballot measure in 1972, the principal argument put before the voters focused on preventing "government and business interests from collecting and stockpiling unnecessary information

---

210. *Id.* at 658.

211. *Id.*

212. *Id.* at 654. "Legally recognized privacy interests are generally of two classes: [1] interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and [2] interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ('autonomy privacy')." *Id.*

213. *Id.* at 657.

214. Dichter & Burkhardt, *supra* note 92, at 46.

215. Regular surveys of expectations to privacy in the workplace correlated with demographic data could help policy makers address this issue.

about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us."[216] The world of work for many people today is a clear indication that the constitutional right to privacy adopted by California voters over fifty years ago, at least as interpreted by the court, has failed to fully prevent the harms identified by the proponents of the ballot measure.

3. *Collective Rights to Privacy*

In 2022, Jennifer Abruzzo, Chief Counsel for the National Labor Relations Board (NLRB or "the Board"), issued a memorandum outlining the state of electronic monitoring in workplaces and the threat that the implementation of monitoring practices poses, without any other action by the employer that would indicate they could be engaged in unlawful surveillance, to employees' rights under section 7 and section 8 of the National Labor Relations Act.[217] Broadly speaking, and among other things, section 7 protects employees' rights to engage in collective action, while section 8 makes it unlawful for employers to "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 7 . . . ." The Board has long held that surveillance is itself coercive and restricts worker organizing.[218] An impression of surveillance created by an employer, even without proof of actual surveillance, is enough to violate the Act.[219]

> The idea behind finding "an impression of surveillance" as a violation of Section 8(a)(1) of the Act is that employees should be free to participate in union organizing campaigns without the fear that members of management

216. White v. Davis, 533 P.2d 222, 233–34 (Cal. 1975) (en banc); *see also Hill*, 865 P.2d at 642 ("At present there are no effective restraints on the information activities of government and business. . . . The proliferation of government and business records over which we have no control limits our ability to control our personal lives . . . .") (emphasis removed).

217. Memorandum from Jennifer A. Abruzzo, *supra* note 16, at 1; *see also* National Labor Relations Act, 29 U.S.C. §§ 157, 158. Also, note that the Act only protects employees, not independent contractors. Memorandum from Jennifer A. Abruzzo, *supra* note 16, at 1.

218. *See, e.g.*, Mitchell Plastics, Inc., 159 N.L.R.B. 1574 (June 27, 1966) (finding that while an employer's actions "did not constitute unlawful surveillance, his comments to the employees about these observations were entirely unnecessary and plainly created an impression of surveillance" in violation of the Act); Ste-Mel Signs, Inc., 246 N.L.R.B. 1110 (Dec. 14, 1979) (concluding that "creating the impression that employees' union activity was under surveillance" violated the Act).

219. Flexsteel Indus., 311 N.L.R.B. 257 (May 28, 1993); *see also* Haynes Motor Lines, Inc., 273 N.L.R.B. 1851, 1855 (Feb. 8, 1985) ("Thus, the Respondent's statements that they are aware of the employees that are pushing the Union, clearly conveys to the employees that their union activities are under surveillance and clearly create the impression of surveillance. Such conduct is clearly coercive and clearly intimidates the employees in the exercise of their rights guaranteed by Section 7."); Emerson Elec. Co., 287 N.L.R.B. 1065, 1070 (Jan. 18, 1988).

> are peering over their shoulders, taking note of who is involved in union activities, and in what particular ways.[220]

Electronic monitoring practices may create an unlawful impression of surveillance. In April of 2023, the Board decided a case against a trucking company that engaged in electronic monitoring without what the Board considered to be a sufficient legitimate business reason.[221] A driver had covered the camera in the cabin of his truck during his lunch break and his manager texted him telling him covering the camera went against company rules.[222] The trial examiner had dismissed the case, finding that the presence of the camera meant that a manager accessing the camera was not "out of the ordinary."[223] That is, the conspicuous presence of the monitoring device created a reasonable expectation that the space was not private. On appeal, the Board ordered the company to cease from such activities because they created an impression of surveillance.[224]

General Counsel Abruzzo advocates for creating a presumption that employer electronic monitoring practices that "viewed as a whole, would tend to interfere with or prevent a reasonable employee from engaging in activity protected by the Act" would violate section 8(a)(1).[225] If employers show that they have no other means to meet their legitimate business needs, such as for facility security, then the balance of the employee and employer interests would be weighed to determine whether the monitoring is appropriate.[226] This would still require judges to engage in a fact-heavy analysis of monitoring practices to determine whether they would prevent reasonable employees from engaging in protected activities. But it extends privacy protections beyond the common law and constitutional rights by centering employee reactions to monitoring practices themselves, rather than focusing first on the nature of the information collected and its use; and it would do so on a national level. However, where monitoring practices only implicate individual harms, this presumption would not add protections for workers. This would be the case where the primary impact of monitoring is stress felt by individuals to meet a quota rather than surveillance concerns, or where workers do not expect to engage in activities protected under the Act because they are properly classified as independent contractors.

220. Flexsteel Indus., 311 N.L.R.B. 257, 257 (May 28, 1993).
221. Stern Produce Co. & United Food & Com. Workers, Local 99, 372 N.L.R.B. 1, 2 (Apr. 11, 2023).
222. *Id.*
223. *Id.*
224. *Id.*
225. Memorandum from Jennifer A. Abruzzo, *supra* note 16, at 8.
226. *Id.* at 7–8.

4. *California Statutory Protections for Rights to Privacy and Autonomy in the Workplace*

California does not have a comprehensive law governing employer electronic monitoring practices. Rather, to address specific risks regarding employer use of worker personal information and to protect workers' bodily autonomy, California has, over several decades, adopted numerous statutes to expand upon the common law and constitutional privacy rights of workers. Five years before the voters of California adopted the right to privacy as a constitutional amendment, the legislature passed the Invasion of Privacy Act:

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.
>
> The Legislature by this chapter intends to protect the right of privacy of the people of this state.[227]

This law, along with legislation throughout the years following, codified, explicated, and expanded many of the common law protections in the state.[228]

By passing laws targeting specific employer practices of data collection and use, the legislature has made policy determinations for the proper balance between a worker's reasonable expectation of privacy in the collection and use of specific types of information and an employer's legitimate business interests. The California Fair Chance Act protects job applicants from having to reveal their conviction history prior to an offer being made.[229] The legislature thereby balances worker and employer interests by limiting the context in which this data can be used by the employer without prohibiting its legitimate uses—employers may only consider conviction history after independently making a determination about the fitness of a candidate based on other data points the employer deems important to the decision. The California Consumer Reporting Agencies Act similarly protects job applicants and employees against an employer's use of the worker's credit history, unless there is a legitimate business need to do so, like for positions dealing with large amounts of cash or other people's personal credit information.[230] Social media usernames,

227. CAL. PENAL CODE § 630 (West 2005).

228. *Id.* § 637.2 (allowing for a civil action and penalty of $5,000 per violation of Penal Code sections 631–632 and 635, prohibiting unauthorized access of phone calls and recorded messages (i.e., wiretapping), regardless of actual damages).

229. CAL. LAB. CODE § 432.7 (West 2022).

230. CAL. CIV. CODE § 1785.20.5 (West 2012); *id.* § 1024.5 (West 2015); *Credit Reports and Background Checks*, LEGAL AID AT WORK, https://legalaidatwork.org/factsheet/credit-reports-and-background-checks (last visited Apr. 19, 2024).

passwords, and content are protected from coerced disclosure, unless they are implicated in an investigation into misconduct.[231] However, employers may request social media usernames and passwords to the extent they are necessary to access a device owned by the employer.[232] The Confidentiality of Medical Information Act regulates consent for disclosure of medical information.[233] Employers are prohibited from monitoring and recording audio and video in locker rooms and restrooms.[234]

Decisions based on inferences drawn from electronic monitoring may implicate discrimination concerns. The Fair Employment and Housing Act prohibits:

> any nonjob-related inquiry of an employee or applicant . . . that expresses, directly or indirectly, any limitation, specification, or discrimination as to race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, reproductive health decisionmaking, or veteran or military status . . . .[235]

With limited exceptions for business necessity, meaning the person's ability to do the job, the act prohibits any employer from "requir[ing] any medical or psychological examination . . . any medical or psychological inquiry [or making] any inquiry [into] whether an applicant has a mental disability or physical disability or medical condition . . . ."[236]

Perhaps there is value in applying this "Swiss cheese" approach to regulating workplace privacy; many laws include broad but vague guiding principles that leave holes in privacy protections for the courts to attempt to fill through interpretation. Still, layered together (like slices of Swiss cheese), these laws may prove more effective than attempts at passing omnibus legislation to provide more comprehensive coverage.[237] Still, it seems that pervasive electronic monitoring has found its way through the gaps in between the myriad laws regulating workplace privacy and worker autonomy. Despite repeated policy statements by the legislature and the people of California through ballot

---

231. LAB. § 980.

232. *Id.*

233. CIV. § 56.20(c).

234. LAB. § 435(a).

235. CAL. GOV. CODE § 12940(d) (West 2023).

236. *Id.* § 12940(e)(1).

237. *See* Shawn Hubler, *California Has America's Toughest Gun Laws, and They Work*, N.Y. TIMES (May 31, 2022), https://www.nytimes.com/2022/05/31/us/california-gun-laws.html. In assessing the success of California's many gun control laws, "results for one policy might be mixed or even negative. But what California has done over a number of decades has been to enact a whole bundle of policies that I think work in synergy, to measurable effect." *Id.* See Siobhan Roberts, *The Swiss Cheese Model of Pandemic Defense*, N.Y. TIMES (Dec. 7, 2020), https://www.nytimes.com/2020/12/05/health/coronavirus-swiss-cheese-infection-mackay.html, for a good graphic depiction of this idea.

measures calling for stronger privacy protections, electronic monitoring has proliferated in workplaces.[238] The California Consumer Privacy Act is the latest attempt to improve privacy protections for Californians. However, even though one of its aims was at addressing harms of excessive electronic monitoring,[239] workers were an afterthought in the law, and it will likely have little impact in this regard.

B. PROTECTIONS BASED ON PROPERTY RIGHTS IN COLLECTED DATA—THE CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act (CCPA) was initially crafted as a ballot measure by Alastair Mactaggart.[240] Mactaggart provided the early funding to place the initiative on California's November ballot in 2019 as Proposition 24.[241] After extensive business lobbying, he agreed to withdraw the measure and the law was passed by the legislature.[242] Originally, the bill included workers in its definition of "consumer," but it was amended after passage to exempt workers from its protections for one year.[243] "[S]takeholders agreed to a sunset to both exemptions in order to encourage discussions around how best to address employer and employee data privacy issues . . . ."[244] When those discussions failed to happen, the original proponent introduced a new

238. *See supra* Part I.B.

239. Issie Lapowsky, *Inside the Closed-door Campaigns to Rewrite California Privacy Law, Again*, PROTOCOL (Feb. 6, 2020), https://www.protocol.com/inside-california-privacy-law-redo [https://web.archive.org/web/20240218082234/https://www.protocol.com/inside-california-privacy-law-redo].

240. John Woolfolk, *SV Chat: Alastair Mactaggart Talks About New Data Privacy Law, Plan to Strengthen It*, MERCURY NEWS (Jan. 27, 2020, 11:48 AM), https://www.mercurynews.com/2020/01/20/sv-chat-alastair-mactaggart-talks-about-new-data-privacy-law-plan-to-strengthen-it/; Brian Fung, *The Unlikely Activist Behind the Nation's Toughest Privacy Law Isn't Done Yet*, CNN BUS. (Oct. 10, 2019, 10:12 AM EDT), https://www.cnn.com/2019/10/10/tech/alastair-mactaggart/index.html ("[H]e told CNN it was 'literally a shower thought' that led him to marry the two ideas [of data privacy and ballot initiatives], paving the way for a landmark California law regulating apps, websites and tech companies that could set a precedent for the rest of America.").

241. Ben Adler, *California Passes Strict Internet Privacy Law with Implications for the Country*, NPR (June 29, 2018, 5:05 AM ET), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country.

242. *Id.*; Gilad Edelman, *The Fight over the Fight Over California's Privacy Future*, WIRED (Sept. 21, 2020, 9:00 AM), https://www.wired.com/story/california-prop-24-fight-over-privacy-future.

243. California Consumer Privacy Act of 2018, A.B. 25, 2019-2020 Sess. (Cal. 2019), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB25&firstNav=tracking.
Many other amendments were offered after passage of the CCPA, weakening the rights provided by the bill. Hayley Tsukayama, *California's Senate Judiciary Committee Blocks Efforts to Weaken California's Privacy Law*, ELEC. FRONTIER FOUND. (July 10, 2019), https://www.eff.org/deeplinks/2019/07/californias-senate-judiciary-committee-blocks-efforts-weaken-californias-privacy.

244. *California Privacy Rights Act: Employee and Business-to-Business Information Must Be Permanently Exempted from Privacy Rights Act to Avoid Unintended Consequences*, CAL. CHAMBER COM. ADVOC. (Jan. 2024), https://advocacy.calchamber.com/policy/issues/california-privacy-rights-act [hereinafter *Employee and Business-to-Business Information*].

ballot measure intended to strengthen and entrench the protections of the original initiative against business lobbying to erode them.[245] Because the California Privacy Rights Act (CPRA) was passed as a ballot measure, any amendments made by the legislature must serve the intent of the measure to protect the privacy of consumers, including workers.[246]

Mactaggart would have made the exemption for employees permanent.[247] Following publication of the first draft of the measure, "Mactaggart met with representatives of the California Labor Federation and the California Employment Lawyers Association, who stressed that workplace surveillance was a pervasive problem. Together, they landed on a three-year exemption for employers, rather than an indefinite one."[248] As it stands, the law defines "consumer" as any natural person who is a resident of California, without a blanket exception for workers.[249] The CPRA's section 3.A.8 explains:

> The privacy interests of employees and independent contractors should also be protected, taking into account the differences in the relationship between employees or independent contractors and businesses as compared to the relationship between consumers and businesses. In addition, this law is not intended to interfere with the right to organize and collective bargaining under the National Labor Relations Act. It is the purpose and intent of the Act to extend the exemptions in this title for employee and business to business communications until January 1, 2023.[250]

The specific rights CPRA confers to California consumers include the rights to: delete personal information;[251] correct inaccurate personal information;[252] know what personal information is being collected and access personal information;[253] know what personal information is sold or shared and

245. Edelman, *supra* note 242; *see also* Fung, *supra* note 240 ("Mactaggart told CNN his new ballot initiative is meant to build a moat around the fledgling CCPA, out of concern that companies opposed to tougher privacy rules will eventually chip away at the consumer protections."); The California Privacy Rights Act of 2020, Proposition 24 in the Nov. 2020 Gen. Election, Sec. 2.D. ("Even before the CCPA had gone into effect, the Legislature considered many bills in 2019 to amend the law, some of which would have significantly weakened it. Unless California voters take action, the hard-fought rights consumers have won could be undermined by future legislation.").

246. People v. Kelly, 222 P.3d 186, 197, 208, 211 (Cal. 2010) (determining that the legislature may propose amendments to initiatives to be adopted by referendum, may legislate on the same subject matter if those laws do not affect the initiative, and may amend the initiative if doing so does not detract from it or alter its purpose).

247. Lapowsky, *supra* note 239.

248. *Id.*

249. CAL. CIV. CODE § 1798.140 (West 2024).

250. The California Privacy Rights Act of 2020, Proposition 24 in the Nov. 2020 Gen. Election, Sec. 3.A.8.

251. CIV. § 1798.105.

252. *Id.* § 1798.106.

253. *Id.* § 1798.110.

to whom;[254] opt out of sale or sharing of personal information;[255] limit use and disclosure of sensitive personal information;[256] and not face retaliation following opt out or exercise of other rights.[257] Collection of data is allowed by default, requiring individuals to opt-out rather than opt-in to data collection.[258]

The law provides exemptions for workers when they act in the scope of employment.[259] Crucially, in relation to electronic workplace monitoring, a key exemption states that the rights conferred by CPRA do not apply to:

> Personal information that is collected by a business about . . . an employee . . . or independent contractor of, that business to the extent that the . . . personal information is collected and used by the business solely within the context of the . . . role as a job applicant to, an employee of . . . or an independent contractor of, that business.[260]

This makes sense considering the nature of the law as a consumer protection statute—the relationship between a worker and employer, based in agency, is different from the more transactional relationship between a business and a consumer. But this means that the law will be ineffective at diminishing the harms of excessive workplace electronic monitoring because of the breadth of the language of the exception.

In reality, though consumers have the right to ask businesses to fulfill requests based on these rights, business may easily find reasons to deny requests.[261] These include arguments that the information is necessary to comply with legal obligations or the ability of the business to defend legal claims. In the case of worker requests, businesses will likely often claim that information was collected solely within the scope of the employment relationship.[262] The refusal

254. *Id.* § 1798.115.

255. *Id.* § 1798.120. This is the source of the warning about cookies and the option to opt-out when visiting many websites. *Frequently Asked Questions (FAQ)*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/faq.html (last visited Apr 20, 2024).

256. CIV. § 1798.121.

257. *Id.* § 1798.125.

258. CAL. PRIV. PROT. AGENCY, *supra* note 255.

259. CIV. § 1798.145(m)–(o).

260. *Id.* § 1798.145(m)(1)(a).

261. CAL. PRIV. PROT. AGENCY, *supra* note 255.

262. *See* Zoe Argento, *California Privacy Rights Act for Employers: The Rights to Know, Delete, and Correct*, LITTLER MENDELSON P.C. (Aug. 16, 2021), https://www.littler.com/publication-press/publication/california-privacy-rights-act-employers-rights-know-delete-and-correct ("First, the right to delete applies to personal information only "collected from" the individual. This appears to mean that the CPRA exempts from the right to delete a wide array of personal information that the employer creates about the HR Individual or receives from other sources, rather than receiving from the HR Individual. . . . Second, an employer may refuse a request to delete as necessary to comply with other laws applicable to the employer. . . . Third, the organization can refuse a request to delete if deleting the data would prevent the business from exercising or defending legal claims. . . . [These] limitations . . . should provide grounds for most employers to reject the majority of requests.") (emphasis omitted). The author goes on to list many other exceptions and limitations to

of businesses to refuse worker requests under CCPA rights makes any employer notice and worker consent meaningless. Further, where businesses fail to take required actions, CCPA does not create a private right of action for most violations, unless a data breach has occurred.[263] Workers also cannot bring suit under the Private Attorneys General Act (PAGA).[264] Rather, the CPRA established the California Privacy Protection Agency (CPPA) and tasked it with enforcing the California Consumer Privacy Act by investigating complaints and levying fines where appropriate.[265]

CCPA only applies to businesses with "gross annual revenue of over $25 million" unless the business is specifically engaged in transacting in personal information, either by buying, selling, or sharing the information of 100,000 or more *California residents* or by making half of its revenue from "selling or sharing *California residents*' personal information."[266] The CCPA does not apply to non-profits or government agencies.[267]

Californians for Consumer Privacy, the Mactaggart-led group behind Proposition 24, made many of the same arguments in favor of the proposition as were made in support of the 1972 ballot measure that enshrined the right to privacy in the state constitution. However, in advocating for the measure on the basis of workers' interests, however, the group overstated the likely impact of the law, which either merely replicated existing protections or failed to fill gaps in existing law to better protect workers. For example, the group stated that "Prop 24 would make it easier for workers to organize by protecting their sensitive personal information, *including union membership*. No more tracking union organizers, firing activists, or interfering with the right to organize and collective bargaining."[268] But the NLRA already protected against tracking where there is an impression of surveillance and the CCPA does not preclude job related tracking. The group also stated that "Prop 24 forbids retaliation against 'an employee, applicant for employment, or independent contractor' for exercising their privacy rights, unlike existing law."[269] At the time of CPRA's

---

the rights granted by CCPA. *See also* Jason C. Gavejian & Joseph J. Lazzarotti, *The Year Ahead in Expanding Privacy Laws: CCPA/CPRA, AI, Electronic Surveillance*, JACKSON LEWIS (Jan. 23, 2023), https://www.jacksonlewis.com/podcast/year-ahead-expanding-privacy-laws-ccpacpra-ai-electronic-surveillance.

263. CAL. PRIV. PROT. AGENCY, *supra* note 255.

264. CAL. LAB. CODE § 2699.5 (West 2020).

265. CAL. PRIV. PROT. AGENCY, *supra* note 255.

266. *Id.* (emphasis added).

267. *Id.*

268. *Id.*

269. *Id.*

passage, many laws already protected against retaliation for complaints about invasions of privacy.[270]

The Los Angeles Times editorial board supported Proposition 24, likening its stricter privacy protections to the European General Data Protection Regulation (GDPR), and finding that the changes would make a meaningful difference and that as a ballot measure it would prevent the erosion of privacy rights by the legislature.[271] The Electronic Privacy Information Center (EPIC) listed several of the benefits of the legislation, including "some data minimization requirements," the creation of the CPPA, closing some loopholes, and the value of passing the law as a ballot measure.[272] However, EPIC highlighted the failure of the measure to expand the private right of action to enforce the law.[273] Privacy Rights Clearinghouse, a San Diego-based data privacy advocacy organization, and San Francisco-based Electronic Frontier Foundation (EFF) similarly both gave ambivalent reviews of the measure, highlighting the limited nature of the law's data minimization protections, the absence of a private right of action, and many other missed opportunities and backwards steps.[274] The San Francisco Chronicle editorial board looked at this ambivalence of major privacy advocates[275] and also recommended a "No" vote.[276]

Opponents of Proposition 24 found the detriments of the law outweighed its utility. The American Civil Liberties Union (ACLU) recommended a "No" vote stating the measure would weaken privacy protections, while focusing

---

270. For example, California Labor Code section 1024.6 provides that an employer "may not discharge an employee or in any manner discriminate, retaliate, or take any adverse action against an employee because the employee updates or attempts to update his or her personal information based on a lawful change of name, social security number, or federal employment authorization document." CAL. LAB. CODE § 1024.6 (West 2015).

271. The Times Editorial Board, *Endorsement: Yes on Prop. 24. It's Not Perfect, but It Would Improve Online Privacy*, L.A. TIMES (Sept. 15, 2020, 3:00 AM PT), https://www.latimes.com/opinion/story/2020-09-15/yes-on-proposition-24.

272. *California's Proposition 24*, ELEC. PRIV. INFO. CTR., https://epic.org/californias-proposition-24 (last visited Apr. 20, 2024). EPIC is a Washington, DC based thinktank that advocates for consumer privacy protections. The organization did not take a position on Proposition 24. *Id.*

273. *Id.*

274. *California Proposition 24: Our Analysis*, PRIVACYRIGHTS.ORG (Oct. 8, 2020) https://privacyrights.org/resources/california-proposition-24-our-analysis; Lee Tien, Adam Schwartz & Hayley Tsukayama, *Why EFF Doesn't Support California Proposition 24*, ELEC. FRONTIER FOUND. (July 29, 2020), https://www.eff.org/deeplinks/2020/07/why-eff-doesnt-support-cal-prop-24.

275. *See* Katy Murphy, *These California Privacy Initiative Opponents Might Surprise You*, POLITICO (July 21, 2020, 5:10 PM EDT), https://www.politico.com/states/states/california/story/2020/07/21/these-california-privacy-initiative-opponents-might-surprise-you-1302560. Some groups did support the measure, including the NAACP of California and Common Sense Media, an organization devoted to protecting children online. *Id.*

276. *Chronicle Recommends: Vote No on Prop. 24, A Flawed Privacy Initiative*, S.F. CHRON. (Oct. 6, 2020, 4:14 PM), https://www.sfchronicle.com/opinion/editorials/article/Chronicle-recommends-Vote-no-on-Prop-24-a-15598736.php.

primarily on the law's "opt-out" structure for collecting personal information.[277] This is a key point in relation to electronic workplace monitoring—an opt-in structure would preclude employers from collecting protected information without a worker's consent. Following the passage of Proposition 24, the ACLU made sure to point out that voters intended to strengthen privacy protections in the state and recommended that the legislature work to fill in the gaps in the law to meet that intent.[278]

CCPA, the first law of its kind in the United States, has at times been described as a California version of the European Union's GDPR and other international laws that provide robust protections for both consumers and workers.[279] However, these laws are not a silver-bullet for workers trying to protect their privacy and autonomy interests against pervasive electronic monitoring practices because they are designed to protect consumers.[280] The "basic presumptions about how workers and consumers are not remunerated for the data that they provide to firms is correct, [the] solution—to pay them for it—raises more problems than it solves."[281]

The on-demand labor context has closer parallels between worker and consumer interests than in other industries with less transactional workplaces. "[P]ersonalized wage[s] [are] determined through an obscure, complex systems that make it nearly impossible for workers to predict or understand their constantly changing, and frequently declining, compensation."[282] The recent rapid growth of monitoring in many higher-wage "white-collar" workplaces[283] foreshadows the application of productivity analytics used in the on-demand sector as employers attempt exercise greater control of their workforces, both in terms of behaviors and costs.[284] Until these more "intellectual" jobs resemble

277. *ACLU of Northern California Statement on Prop. 24*, ACLU N. CAL. (Nov. 4, 2020), https://www.aclunc.org/news/aclu-northern-california-statement-prop-24; Jacob Snow & Chris Conley, *Californians Should Vote No on Prop 24*, ACLU N. CAL. (Oct. 16, 2020), https://www.aclunc.org/blog/californians-should-vote-no-prop-24.

278. *ACLU of Northern California Statement on Prop. 24*, *supra* note 277.

279. *See e.g.*, Alvin Velazquez, Kim Campion & Carrie Dove Storer, *Workplace Privacy Around the Globe*, *in* A.B.A. SECTION LAB. & EMP. L., NAT'L SYMP. ON TECH. IN LAB. & EMP. L. (Apr. 6–8, 2016), https://www.americanbar.org/groups/labor_law/committees/techcom/tech_archive/2016; *see also* Olivier Proust, *The Risks of Online Employee Monitoring During the COVID-19 Crisis*, FIELDFISHER (Apr. 14, 2020), https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/the-risks-of-online-employee-monitoring-during-the.

280. Dubal, *supra* note 65, at 1979–80, 1983–84, 1986. *But see* Morgan Sullivan, *Managing Employee DSAR Under CPRA [2023 Guide]*, TRANSCEND (Jan. 6, 2023), https://transcend.io/blog/employee-dsar/#challenges ("The main takeaway from GDPR precedent is that employers most commonly receive access requests during pre-litigation or a pre-dispute process. A terminated employee or disgruntled job applicant may look to leverage these privacy rights as a form of free discovery.").

281. Dubal, *supra* note 65, at 1986.

282. *Id.* at 1936.

283. *See* discussion *supra* Part I.

284. *See* Kantor & Sundaram, *supra* note 25.

the transactional nature of consumer–business interactions like in the on-demand sector, laws like CCPA will not provide recourse against excessive monitoring. In this context, workers will have to wait for the quality of their jobs to erode to receive protections under the law.

CCPA is built on the idea that the exchange of information between consumers, including workers, and businesses is transactional, that data is property.[285] The drafters believed that by conferring the right to access their own information, consumers could properly put a monetary value to relinquishing control over their personal data.[286] The law was primarily crafted to create more balance in the property rights to data between consumers and businesses that would enable market-based solutions to data privacy problems.

Legal scholars and judges must exercise caution when attempting to discern voter intent from a proponent's arguments in favor of a ballot measure.[287] It is not clear voters specifically adopted the view of the measure's proponents that the best way to protect worker privacy relied on free market principles. However, when looking at the findings in the CPRA in relation to the arguments put before voters, one message is clear: California voters wanted to strengthen their constitutional right to privacy.

III. STRONGER PROTECTIONS AND MORE ENFORCEMENT ARE NEEDED TO PROTECT CALIFORNIA WORKERS FROM EXCESSIVE ELECTRONIC MONITORING PRACTICES IN TODAY'S WORKPLACES

> "As we consider how technology has assisted the employer in controlling workers, we must also look at how the law has played unwitting accomplice in the domination of workers."[288]

Something often lost in this legal discourse is the actual experience of workers. Even where a legitimate business interest exists for some monitoring, to increase productivity for example, excessive electronic monitoring can harm workers, and particularly, vulnerable workers. "[T]he rising use of intrusive monitoring and management technologies disproportionately affects low-wage workers, workers of color, immigrants, and women, who are more likely to work in heavily tracked positions in warehousing, package delivery, and call centers." Protections need to take into account worker experiences of monitoring that

285. The California Privacy Rights Act of 2020, Proposition in the Nov. 2020 Gen. Election, Sec. 2.F.

286. *Id.* ("This asymmetry of information makes it difficult for consumers to understand what they are exchanging and therefore to negotiate effectively with businesses."); *id.* at Sec. 2.G–I ("Absent these tools, it will be virtually impossible for consumers to fully understand these contracts they are essentially entering into when they interact with various businesses.").

287. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 644 (Cal. 1994) ("[S]uch vague and all-encompassing terms afford little guidance in developing a workable legal definition of the state constitutional right to privacy.").

288. AJUNWA, *supra* note 24, at 30.

allow for differences in workplace contexts and do not just default to a projection of the average worker.

Companies might be convinced to not monitor workers for ethical reasons or business reasons, such as system costs, reduced morale, or worker distraction.[289] But this tenuous possibility is cold comfort to workers who are without sufficient legal protections to challenge existing overly broad electronic monitoring practices. Many law firms and privacy advocates have publicly shared general guidelines for employers implementing monitoring systems. For example, Skadden, Arps, Slate, Meagher & Flom LLP, warns of the potential for "invasion of privacy, unfair labor practice charges, discrimination, unpaid wages and overtime and workplace injuries."[290] Skadden notes how in 2022, the United States Department of Labor issued a fine against a company after finding excessing monitoring led to repetitive stress injuries.[291] Even where the law grants workers some property rights to their data, individual assertion of those rights would almost certainly be of negative value. Where successful, the small awards for individual harms caused by workplace electronic monitoring would likely have a negligible impact on employers' bottom lines. Still, aggrieved workers should individually and collectively challenge excessive electronic monitoring practices in their workplaces under existing privacy protections. In California, public enforcement agencies should investigate and pursue remedies against egregious cases of excessive electronic workplace monitoring under existing legal frameworks.

More study is needed to determine which modern monitoring practices pose the greatest health risks to workers. California should fund those studies and act upon the findings. Still, the prohibition of the most harmful practices, such as algorithmic wage discrimination, and a true opportunity to opt-out of the collection of certain forms of personal information, especially biometric information, is a good place to start. Ultimately, the legislature, or the public

289. Rohan Narayana Murty & Shreyas Karanth, *Monitoring Individual Employees Isn't the Way to Boost Productivity*, HARV. BUS. REV. (Oct. 27, 2022), https://hbr.org/2022/10/monitoring-individual-employees-isnt-the-way-to-boost-productivity; Jared Newman, *Why Companies Shouldn't Track Everything Their Remote Workers Do Online*, FAST CO. (May 27, 2020), https://www.fastcompany.com/90509420/surveilling-employees-who-work-from-home-could-do-more-harm-than-good; Aytekin Tank, *Tracking Employees Doesn't Work. Here's How to Move Beyond Productivity Paranoia*, FAST CO. (Jan. 11, 2023), https://www.fastcompany.com/90830873/tracking-employees-doesnt-work-heres-how-to-move-beyond-productivity-paranoia; Bart Ziegler, *Should Companies Track Workers With Monitoring Technology?*, WALL ST. J. (Aug. 20, 2022, 11:00 AM ET), https://www.wsj.com/articles/companies-track-workers-technology-11660935634.

290. Annie Villaneuva Jeffers & Crystal D. Barnes, *Every Move You Make: When Monitoring Employees Gives Rise to Legal Risks*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (Sept. 2022), https://www.skadden.com/insights/publications/2022/09/quarterly-insights/every-move-you-make.

291. *Id.*

through future initiatives, should enact comprehensive rules specifically governing workplace electronic monitoring.

A. OPPORTUNITIES TO PROTECT WORKERS UNDER EXISTING LEGAL FRAMEWORKS

1. *Expanded Public Law Enforcement Through Existing Legal Frameworks*

The passage of the CCPA did not fundamentally change the paradigm that allows for excessive monitoring in workplaces, but it can still be a weapon in the arsenal of those wishing to challenge such practices as inherently harmful. The Governor should ensure the CPPA is adequately funded and staffed to process claims that employers have violated workers' privacy rights and should publicize findings of violations and fines levied by the CPPA to ensure the issue of data mismanagement remains in the public eye. The Attorney General ("AG") also has the authority to enforce the provisions of the CCPA and has shown a willingness to do so in a way that takes an expansive view on the rights conferred by the law.[292] Accordingly, the AG should take a limited view of exemptions granted for employers limiting workers' rights under that law, in accordance with the directive under CCPA for liberal construction of the law.[293] In July 2023, AG Bonta began soliciting information from large employers about their efforts to comply with the portions of CCPA applicable to employees.[294]

District Attorneys, City Attorneys, and the State AG could make use of the State's Unfair Competition Law ("UCL") where certain electronic monitoring practices harm competition.[295] City or county counsel could bring suit for unfair competition related to excessive or deceptive electronic monitoring.[296]

---

292. California Consumer Privacy Act, 105 Ops. Cal. Att'y. Gen. 26, at 11–13, 14–15 (2022) (finding that the statutory text and legislative intent behind CCPA show that internally drawn inferences about consumers are covered as personal information). This seems to indicate data about workers purchased by a business from data brokers would be covered by the law. Even so, the Delete Act, currently pending legislation, would allow consumers, through the CPPA, to direct all data brokers operating in the state to delete the consumer's personal information they hold. Data Broker Registration: Accessible Deletion Mechanism, S.B. 362, 2023–2024 Sess. (Cal. 2023), https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=202320240SB362; *Data Brokers Beware: Californians Will Gain New Privacy Protections Under "The Delete Act"*, JOSH BECKER (Apr. 11, 2023), https://sd13.senate.ca.gov/news/press-release/april-11-2023/data-brokers-beware-californians-will-gain-new-privacy-protections.

293. CAL. CIV. CODE § 1798.194 (West 2019).

294. Press Release, Off. of the Att'y Gen. of Cal., Attorney General Bonta Seeks Information from California Employers on Compliance with California Consumer Privacy Act (July 14, 2023), https://oag.ca.gov/news/press-releases/attorney-general-bonta-seeks-information-california-employers-compliance.

295. CAL. BUS. & PROF. CODE § 17200 (West 1993).

296. *Id.* § 17204. Under the UCL, "unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." *Id.* § 17200.

Prosecutors could, for example, sue an employer for refusing to turn over required documents under CCPA since violations of CCPA are unlawful and a business that is not expending resources to comply with the law gains an unfair advantage against its legally compliant competition. These cases could bolster private actions under other legal theories through discovery and the pressure on employers from the publicity of cases.[297] Cases may be harder to win where the employer's actions are fraudulent or unfair, but, as with most electronic monitoring practices today, remain within the bounds of the law.[298] Still, enterprising public prosecutors, in addition to private parties, could bring cases under this law based on the electronic monitoring industry's own assessment of ethical practices, for example, where an employer has been found to engage in electronic monitoring without disclosure to workers. Other potentially fruitful cases may involve excessive collection of worker data for resale, but not to further the employer's interest in control or security of the workplace. This could present an unfair advantage in competition because the employer could offset some of its labor costs by extracting more value from workers than its competitors that comply with the industry's ethical standards to remunerate workers for the sale of their personal information.

2. *Collective Action Strengthens Protections for Workers Challenging Individual Employer Practices*

NLRB actions to prohibit monitoring where it creates a risk of interfering with organizing activity adds protections for some workers in a meaningful way.

---

297. *Id.* § 17205 ("[T]he remedies or penalties [under the UCL] are cumulative to each other and to the remedies or penalties available under all other laws of this state.").

298. *See* Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co., 973 P.2d 527, 544 (Cal. 1999) ("[T]o guide courts and the business community adequately and to promote consumer protection, we must require that any finding of unfairness to competitors under section 17200 be tethered to some legislatively declared policy or proof of some actual or threatened impact on competition. We thus adopt the following test: When a plaintiff who claims to have suffered injury from a direct competitor's 'unfair' act or practice invokes section 17200, the word 'unfair' in that section means conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition."). *But see* Safeway, Inc. v. Super. Ct., 190 Cal. Rptr. 3d 131, 146 (2015) (noting that there is a difference between statutes not making a practice unlawful and making it lawful, and holding that "[n]othing in *Cel-Tech* suggests that unfairness requires a statutory violation; on the contrary, *Cel-Tech* expressly states that the UCL is independent of other statutes, and prohibits unfair practices not otherwise unlawful. Furthermore, assuming—without deciding—that the test for unfairness set forth in Cel–Tech is applicable to petitioners' claim, the alleged practice is unfair, in view of the Labor Code provisions discussed above regarding timely payment of wages, as well as the public policy they embody." (citations omitted)); s*ee also In re* Google Assistant Priv. Litig., 456 F. Supp. 3d 797, 842–44 (N.D. Cal. 2020). The court discussed State court and Ninth Circuit decisions analyzing the unfair prong of the UCL, and found that there was uncertainty about whether the *Cel-Tech* standard applied. The court ultimately found that plaintiffs failed to allege harm to competition (under the *Cel-Tech* test) but that under prior tests, they should have leave to amend to clarify their invasion of privacy claims, following the balancing test as for the tort under the common law. *Id.*

Even with private-sector union membership at a low of just fifteen percent in California,[299] employees can still engage in less formal collective action to challenge excessive electronic monitoring practices where they have been implemented by an employer. Employees who wish to challenge excessive monitoring practices should organize with their coworkers to enjoy the protections of section 7 of the NLRA.

In the on-demand independent contracting context, data collectives that attempt to match employer power by assembling similar datasets to those that employers maintain, and sharing insights gained among members will likely fall short of their goals because employers retain the greatest value of collected data.[300] Indeed, the datasets assembled by these collectives might only have value to the employer. At a minimum, the market for such specific data is necessarily very limited. "Worse, like other proposals that claim that 'data production is labor', these approaches may reify widespread data collection as a social good, thus ignoring problems of individual and social harms that result from broad surveillance, categorization, and data derivative processing."[301]

3. *Private Litigation: Barriers and Collateral Challenges*

Legal challenges to any workplace electronic monitoring practices under existing legal frameworks in California present significant hurdles for workers.[302] Still, workers can challenge excessive electronic monitoring as an inherent violation of the guarantee in the state constitution of the right to privacy. "[I]f privacy is once recognized as a right entitled to legal protection, the interposition of the courts cannot depend on the particular nature of the injuries resulting."[303] Employment contracts that provide no meaningful alternative to excessive monitoring, meaning workers cannot meaningfully consent to the monitoring, or those contracts that do not disclose monitoring to workers, might be challenged as unconscionable, despite the difficulties in succeeding on those claims.[304]

Arbitration clauses in employment contracts present hurdles for workers bringing cases under existing laws. However, overbroad monitoring practices that invade workers' lives off-the-clock may be subject to challenge, as shown

299. *Future of Work Commission*, *supra* note 48.

300. Dubal, *supra* note 65, at 1986–87.

301. *Id.* at 1986.

302. *See* discussion *supra* Part II.

303. Warren & Brandeis, *supra* note 71, at 205.

304. *See* CAL. CIV. CODE § 1670.5 (West 2023); OTO, L.L.C. v. Kho, 447 P.3d 680, 690 (Cal. 2019) ("The ultimate issue in every case is whether the terms of the contract are sufficiently unfair, in view of all relevant circumstances, that a court should withhold enforcement. The burden of proving unconscionability rests upon the party asserting it.") (citations omitted); *see also* AJUNWA, *supra* note 24, at 387 ("[T]he fact remains that modern contract law recognizes public policy considerations that may trump intent to contract.").

in a recent case in which independent contractors for Amazon claimed the company spied on drivers by monitoring a closed Facebook group without their knowledge.[305] Plaintiffs based their claims in the wiretapping provisions of the penal code, the common law, and the constitutional right to privacy.[306] Amazon sought to force arbitration based on the contract.[307] The court found that "[t]he alleged misconduct would be wrongful even if there had been no contract."[308]

> "Amazon seeks arbitration because the alleged monitoring of drivers' conversations took place while the drivers were performing deliveries for Amazon under the agreement . . . . [But] Amazon's alleged misconduct existed independently of the contract . . . ."[309]

The Amazon case highlights how undisclosed monitoring practices in particular may violate existing laws. Judges and advocates could also explore the application of workplace health and safety laws where disclosed monitoring practices result in harm to worker mental and physical health due to stress.

Perhaps the greatest barrier to challenging excessive electronic monitoring may be workers' own reticence to assert their rights, whether for reasons of fatalism or fear of retribution. Many consumers believe they are being tracked online, even when they are not.[310] Workers could challenge monitoring practices by bringing claims for wrongful discharge where employers base adverse actions on information collected by dragnet monitoring practices, or in retaliation for worker complaints about such practices. California courts have already found that an employee's refusal to submit to an overly invasive drug test implicates a fundamental public policy.[311] The Court in *Hill v. National Collegiate Athletic Association* noted that the ballot arguments in favor of the constitutional right to privacy said that the measure would prevent the practice of collecting

305. Jackson v. Amazon.com, Inc., D.C. No. 3:20-cv-02365-WQH-BGS, 2023 WL 2997031 at *7 (9th Cir. Apr. 19, 2023).

306. Jackson v. Amazon.com, Inc., 559 F. Supp. 3d 1132, 1136 (S.D. Cal. 2021), *aff'd*, D.C. No. 3:20-cv-02365-WQH-BGS, 2023 WL 2997031 (9th Cir. 2023).

307. *Amazon.com, Inc.*, 2023 WL 2997031 at *7.

308. *Id.* at *3.

309. *Id.* at *23–24.

310. Bogost, *supra* note 86.

311. Semore v. Pool, 266 Cal. Rptr. 280, 285 (1990) ("While an employee sacrifices some privacy rights when he enters the workplace, the employee's privacy expectations must be balanced against the employer's interests. . . . We think, however, that there is a public policy concern in an individual's right to privacy. Plaintiff's right not to participate in the drug test is a right he shares with all other employees. In asserting the right, he gives it life. While rights are won and lost by the individual actions of people, the assertion of the right establishes it and benefits all Californians in the same way that an assertion of a free speech right benefits all of us.").

unnecessary data.[312] This "privacy nihilism"[313] seriously degrades protections for consumers based on a reasonable expectation of privacy. Similarly, modern electronic workplace monitoring systems may have already eroded the reasonable expectation workers had to privacy in the workplace when California voters adopted the constitutional amendment protecting privacy in 1972. At that time, proponents saw a threat to privacy in the unnecessary stockpiling of personal information. It would have been hard then to fathom the forms of computerized work and the extent of the attendant monitoring that are common in workplaces today. Because of this, statutory protections for workers that explicitly prevent excessive intrusions into workers' physical spaces and mental states—not just those that provide tweaks to legal presumptions or grants of property interests in data—are necessary to restore expectations to dignity and personal autonomy at work.

B. COMPREHENSIVE LEGISLATION REGULATING WORKPLACE MONITORING IS NEEDED TO REALIZE THE CONSTITUTIONALLY GUARANTEED PRIVACY RIGHTS OF WORKERS IN CALIFORNIA AND PROTECT WORKER DIGNITARY INTERESTS

The California Chamber of Commerce has called for workers to be excluded from CCPA and "if needed" to address workplace privacy separately through the legislative process.[314] The state does need a comprehensive law focused on workplace privacy rights—a law tailored to the workplace context would be better able to balance the interests of workers and employers, and prevent harms and the resulting costs to the parties and to society through lost productivity, than the afterthought of considering workers consumers under the CCPA. Proactive legislation should take into account employers' legitimate interests in control and security and identify acceptable use cases for monitoring and should allow flexibility to prevent stifling innovation in the workplace, but that flexibility should require employers, rather than workers, to bear the risk of withstanding judicial scrutiny.

In her 2023 book, *The Quantified Worker*, legal scholar Ifeoma Ajunwa calls for legislation to create an unwaivable right to "data autonomy" for workers.[315] One option is to create a bright-line rule prohibiting monitoring outside of the work context, without an option for workers to waive that right

312. 865 P.2d 633, 654 (Cal. 1994) ("As the ballot argument observes, the California constitutional right of privacy 'prevents government and business interests from [1] collecting and stockpiling unnecessary information about us and from [2] misusing information gathered for one purpose in order to serve other purposes or to embarrass us.'" (citations omitted)).

313. Bogost, *supra* note 86.

314. *Employee and Business-to-Business Information*, *supra* note 244.

315. AJUNWA, *supra* note 24, at 386–87 (detailing her proposed federal Employee Privacy Protection Act).

through notice and consent.[316] To balance employer and worker interests, certain forms of monitoring, like constant audio and video recording of workers, if not banned, could be considered presumptively harmful.[317] Employers who wish to engage in those practices could be required to show more than a need for productivity, such as a specific factual basis for a reasonable belief the work performed by the monitored worker poses a health or security risk.[318] Because technology changes much faster than the law, legislation should focus on setting a policy for the balance between worker rights and employer interests and allow room for a regulatory agency—the CPPA or the Labor Commissioner—to regularly update rules to reflect new innovations[319] and maintain proportionality between competing interests in evolving contexts.[320]

Biometric data should have the strongest protections for collection because, as the Illinois Biometric Privacy Act (BIPA)[321] points out, unlike other personally identifying information, it cannot be changed.[322] One can get a new social security number, but not (as of yet) a new retina. Definitions of biometric data in the law must also be carefully considered because limiting the scope of what the term covers to specific uses may be too narrow, whereas including all data derived from an individual's body may be so broad it ends up vague and meaningless.[323] CPRA covers biometric information "that is used or is intended to be used . . . to establish individual identity."[324] However, this only includes biometric information in the rights established under the law. BIPA, on the other hand, requires express consent from individuals *before* biometric information is collected, prohibits sale and limits disclosure of biometric information to third-parties, and requires a "reasonable standard of care" for storage of biometric

316. *Id.*

317. A.B. 1651, § 1543(b), 2021–2022 Sess. (Cal. 2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1651.

318. *See e.g.*, *id.* § 1543(b)(5).

319. *See* AJUNWA, *supra* note 24, at 64, 83.

320. Tammy Katsabian, *The Telework Virus: How Covid-19 Has Affected Telework and Exposed Its Implications for Privacy*, 44 BERKELEY J. EMP. & LAB. L. 141, 177–78, 184–85 (2023) (arguing for a proportionality approach to privacy in the remote work context that would "determine[] whether (1) there is a rational connection between the goal being furthered by teleworkers' supervision and the means of accomplishing it, (2) the least restrictive means of achieving the employer's goal were used, and (3) there is a proportionate balance between the social benefit of achieving the employer's goal and the harm that may be caused to the teleworker's and their surroundings' right to privacy."). Katsabian also argues for including worker voices in setting employer privacy policies and for requiring of software providers to design systems that protect monitored users' privacy by default. *Id.*

321. S.B. 1189, 2021–2022 Sess. (Cal. 2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB1189.

322. Tatiana Rice, *When Is a Biometric No Longer a Biometric?*, FUTURE PRIV. F. (May 19, 2022), https://fpf.org/blog/when-is-a-biometric-no-longer-a-biometric.

323. *Id.*

324. *Id.*

information.[325] California should look to the law in Illinois as a model. Additionally, BIPA "contains a private right of action that has allowed courts to decide the boundaries of what technologies should and should not [fall] within the scope of the law," with flexibility as new technologies emerge.[326]

One major challenge is definitional: What qualifies as monitoring or surveillance? To determine how to categorize and regulate different practices, the legislature will need to address, ironically, the issue of the dearth of data on workplace electronic monitoring practices. Requiring employers to file a simple online report on the forms of worker monitoring that they use filed with the CPPA either quarterly or annually would help regulators understand the nature of monitoring practices in the modern workplace. Reporting should be shared among other state enforcement agencies such as the Attorney General's office, the Civil Rights Department, and the Labor Commissioner.

"[E]nsuring that companies actually comply with [information privacy] law is a massive regulatory task that state-level agencies may struggle to keep up with."[327] At the Federal level, Senator Robert Casey, (D-PA), has introduced the Stop Spying Bosses Act of 2023.[328] The bill aims to require disclosure of monitoring, prohibit the collection of certain sensitive data, regulate algorithmic decision making, and establish a regulatory and enforcement agency within the Department of Labor.[329] The Senate has not taken any action on the bill.[330] New York,[331] Connecticut,[332] and Delaware[333] already require employers to disclose monitoring to employees in advance. California considered but ultimately failed to adopt similar protections in 2022. Senator Casey has also called for the creation of "an interagency task force . . . to study and provide recommendations for a whole-of-government approach [with] agencies already examining these issues, including the Federal Trade Commission, the National Labor Relations Board, the Equal Employment Opportunity Commission, the White House Office of Science and Technology Policy, among others."[334] Similar legislation could likely be enacted more easily at the state level, which could then serve as

325. Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/15 (2008), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

326. Rice, *supra* note 322.

327. AJUNWA, *supra* note 24, at 167.

328. Stop Spying Bosses Act, S. 262, 118th Cong. 1st Sess. (2023), http://www.congress.gov/bill/118th-congress/senate-bill/262 (the bill has not seen any legislative action since its introduction in February 2023).

329. *Id.*

330. *Id.*

331. A.B. A1920A, 2019–2020 Sess. (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/a1920/amendment/a.

332. 1998 Conn. Pub. Acts 98-142.

333. DEL. CODE ANN. tit. 19, § 705 (2022).

334. Letter from Bob Casey, U.S. Sen., to The Honorable Joseph R. Biden, President of the United States (Dec. 16, 2022), https://www.casey.senate.gov/news/releases/casey-urges-white-house-to-create-taskforce-to-study-worker-surveillance-technologies.

an example for Federal legislators to assess the viability and impact of these policies.

The California legislature should reconsider the Workplace Technology Accountability Act (WTAA) in future legislative sessions.[335] As Jeffers and Barnes, attorneys at Skadden, Arps, Slate, Meagher & Flom note:

> The Workplace Technology Accountability Act (AB 1651) would have (i) required employers to notify employees in advance of any monitoring and explain how, when and why monitoring technology was being used on the job, (ii) prohibited employers from monitoring employees while off duty or using their personal devices, (iii) allowed employees to view and correct data about themselves, (iv) banned the use of facial recognition technology and (v) prohibited employers from using algorithms to decide if and when an employee is to be disciplined or fired.[336]

The California Employment Lawyers Association (CELA) reported that the legislation was aimed at tailoring the privacy protections promised by CPRA to the workplace, and specifically addressed electronic monitoring practices that became more prominent following the massive shift to work-from-home arrangements in the wake of COVID-19.[337] The bill was also supported by the ACLU, EFF, and many prominent labor unions in the state.[338] It would have required employers to provide an upfront notice that explained why that "specific form of electronic monitoring is strictly necessary . . . and is the least invasive means . . . to accomplish an allowable purpose."[339] Crucially, the legislation would have provided for a private right of action in addition to enforcement by the Labor Commissioner.[340]

Fears about the impact of the bill raised by the Chamber of Commerce largely focus on limitations to an employer's ability to discipline workers for misconduct.[341] Reintroduction of the legislation should take into consideration employers' need to provide a safe, secure workplace, but fears about potential impacts on workplace discipline should not prevent legislative action. The

---

335. This bill was introduced by Assemblymember Kalra in the 2021–2022 legislative session, but it died in committee. As of January 2024, Asm. Kalra has no plans to reintroduce the legislation. (In conversation with Asm. Kalra's staff). *See* Jeewon Kim Serrato, Jerel Pacis Agatep & Jenny Ha, *AB-1651: As 'Workplace' Extends to Our Homes, Can Employers Still Conduct Worker Monitoring?*, CAL. LAWS. ASS'N (July 14, 2022), https://calawyers.org/privacy-law/ab-1651-as-workplace-extends-to-our-homes-can-employers-still-conduct-worker-monitoring.

336. Jeffers & Barnes, *supra* note 290; *see also* AJUNWA, *supra* note 24, at 148–50 (discussing the most problematic aspects of facial recognition software).

337. Serrato et al., *supra* note 335.

338. *Worker Rights: Workplace Technology Accountability Act: Hearing on A.B. 1651 Before the Assemb. Comm. on Lab. & Emp.*, 2021-2022 Leg. Reg. Sess., 13–14 (Cal. 2022).

339. *Id.* at 4–5.

340. *Id.* at 8.

341. Ronak Daylami, *CalChamber Tags AB 1651 as a Job Killer*, CAL. CHAMBER COM.: ADVOC. (Apr. 26, 2022), https://advocacy.calchamber.com/2022/04/26/calchamber-tags-ab-1651-as-a-job-killer.

WTAA would have defined monitoring as "the collection of information concerning worker activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic, or photo-optical system."[342] This definition would likely prove to be too vague, leading regulators or courts to determine the scope. "Information" needs to be more clearly defined with reference to transactions conducted by workers that employers track in the course of business and may incidentally cross reference when conducting analysis over a worker's productivity. A better option would be to define monitoring in terms of purpose, while implicating any means that further that purpose.

I recommend as a definition of monitoring "any electronic means implemented to determine an individual worker's time-on-task, rate of production, quality of performance, or any other metrics intended to assist the employer in making employment decisions regarding the monitored individual or any other worker." This definition would be broad enough to cover monitoring that implicates individual workers' interests in production rates set by the employer, as well as systems that aim to control how workers express their personalities at work. It would also avoid unnecessary burdens on employers that would do little to further worker interests, like opening up all employer business recordkeeping to scrutiny in privacy disputes. By aiming at the purpose of monitoring systems, this definition would better address the adversarial nature of worker and employer interests in worker privacy and autonomy, while leaving room for regulatory and judicial determination of the scope of the law applied to emerging technology.

The state's previous attempts to enshrine data minimization into law have failed because they have focused too much on the actual uses to which data is put, and not enough on the process of and purpose for its collection.[343] Similar to the European Union since 1995,[344] the State should require companies prove they have a legitimate business purpose for their monitoring practices before employees file complaints, as proposed in the WTAA.[345] For example, the State could enact requirements similar to those in A.B. 701 that was signed into law in 2021 mandating employer notice to employees of quotas used at large warehouses that may result in employees being unable to comply with meal and

342. A.B. 1651, § 1543(b), 2021–2022 Sess. (Cal. 2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1651.

343. *See* discussion *supra* Part II. *See also* Dubal, *supra* note 65, at 1979 n.214 ("Data abolition at work . . . is an objective that would prevent the ubiquitous extraction of digital data on workers—whether that data is extracted to control labor individually or collectively.").

344. Lokke Moerel, *Workplace Discrimination and Equal Opportunity*, FUTURE PRIV. F. (Feb. 9, 2023), https://fpf.org/blog/workplace-discrimination-and-equal-opportunity.

345. Jeffers & Barnes, *supra* note 290.

rest break and occupational safety and health requirements.[346] The Workplace Technology Accountability Act would have further required employers to offer a limited opt-out option when monitoring is not restricted to data security and other specified purposes, balancing employer and worker interests.[347] CCPA could be read to cover this type of notice requirement, but the law's wording is vague.[348] Future regulations and caselaw will establish the scope of the notice requirements under that law, but the legislature should also proactively address the issue.

To be effective, this type of legislation would need to have robust protections against retaliation.[349] Such a law should also include the option for workers to file complaints with an administrative agency capable of adjudicating the claim, in addition to a private right to sue without the need to exhaust the administrative process. There is strong precedent for this type of adjudicative process in the Labor Commissioner wage claim process. However, workers face years long wait times when bringing wage claims before the labor commissioner.[350] Whether public enforcement is housed at the CPPA or the Labor Commissioner, adequate funding and staffing should be provided for in the law. In addition, these claims should be open to PAGA suits to prevent sidestepping liability through the use of arbitration agreements. If the State legislature fails to pass these protections, privacy advocates should come together to craft a comprehensive law to be passed as a ballot measure that would establish principles for the governance of privacy at work. Proposition 24 passed in 2020 with fifty-six percent of the vote, despite its flaws and a divided privacy community. An initiative crafted by a unified community of privacy advocates could succeed at making substantial changes by setting guidelines, expanding the mandate of the CPPA, and requiring robust regulations to protect workers—and critically, shield those protections from erosion by a future legislature.

IV. CONCLUSION

The law today allows employers to subject workers to an extreme level of scrutiny in all aspects of the working relationship and risks workers' personal data integrity beyond the ever-more-blurry confines of the employment relationship. One challenge for protecting workers' privacy interests is the

346. A.B. 701, 2021–2022 Sess. (Cal. 2021), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB701*; see also* CAL. LAB. CODE § 2101 (West 2022).

347. Serrato et al., *supra* note 335.

348. *See* CAL. CIV. CODE § 1798.110(c) (West 2018).

349. For comparison, the state recently enacted a rebuttable presumption of unlawful retaliation for adverse actions under the new unsafe warehouse quota law. CAL. LAB. CODE § 2105 (West 2022).

350. Farida Jhabvala Romero, *State Wage-Theft Investigators Say Staffing Crisis Is Hurting the Agency*, KQED (July 18, 2023), https://www.kqed.org/news/11955920/california-wage-theft-investigators-staffing-crisis.

inadequacy of contracts in an imbalanced labor market to prevent employer overreach. Relying on torts, workers must wait to recover damages after harms occur rather than acting proactively to address risks.[351] Another challenge for workers attempting to protect their interests in freedom from excessive electronic monitoring under current law is articulating the specific harm done. Continued research and public debate are needed on this issue. But when many workers are subject to unrestrained electronic monitoring in the workplace, the degradation of individuals' ability to establish their own identities and control how they express their personalities is surely a public harm; even if the effective harm to any one individual is miniscule, the sum of the diffuse effects of these unrestrained practices may be substantial.

Unchecked electronic workplace monitoring practices are creating a new paradigm for the relationship between workers and employers. To remedy this situation, solutions should be layered. Individuals and public law enforcement agencies should argue for extending current laws to cover modern excessive electronic monitoring practices. Workers should also collectively pursue their interests directly with their employers. Perhaps most importantly, the legislature should address the specific issue of excessive monitoring and collection of worker data with a comprehensive law aimed at preventing, rather than just redressing harms. The legislature should ban the most harmful practices, but it should further make employers internalize the costs of the harms they cause when they engage in excessive monitoring by shifting the presumption of harmfulness to the employer. In doing so, the legislative process should be careful not to stifle innovation in the internal governance of workplaces. It should consider employers' legitimate business interests in protecting their assets, limiting liabilities and costs, and generating profits. Forward-looking legislation specifically aimed at protecting worker interests in balance with employer interests is needed to ensure workplaces are safe and healthy for workers into the future, and to restore the expectation all Californians should enjoy in a minimum standard of privacy and personal autonomy at work.

351. Warren & Brandeis, *supra* note 71, at 210.