Hastings Communications and Entertainment Law Journal

Volume 44
Number 2 *Spring 2022*

Article 4

Spring 2022

From Utilitarianism to Fordism: How Americans Brought the Panopticon Home

Katherine Hoppe

From Utilitarianism to Fordism: How Americans Brought the Panopticon Home

BY KATHERINE HOPPE*

ABSTRACT

The COVID-19 pandemic forced many not considered essential employees into their homes. Many employers worried about employee accountability, leveraged surveillance techniques to maximize employee performance and ensure productivity. These technologies include screen monitoring software, video recordings of employees within their homes, monitoring of social media, and typing efficiency. While employees continue to work outside of the office, private employers will increasingly monitor employees in spaces traditionally considered private—including the home. As private and public life spheres continue to overlap, privacy for workers may erode. What kinds of surveillance have employees experienced in their homes since the Covid-19 lockdown orders? Moreover, what existing protections do they have? I argue that new legal regimes are necessary to stop the threat of more invasive surveillance techniques. This article outlines the history of surveillance in the workplace and employees' existing protections. Using a comparative perspective, I then examine the legal regulations available to protect employees' privacy in other nations. I conclude that some of these laws may be imported into the U.S. context to ensure employee privacy and well-being.

* Katherine Hoppe is a class of 2022 J.D. candidate at the University of California, Hastings. She received her B.A. in History at Colgate University. Her studies currently focus on Employment and Labor Law.

TABLE OF CONTENTS

I. INTRODUCTION

"He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjugation." – Michel Foucault[1]

Under capitalism, labor surveillance is synonymous with efficiency. Whether in an office or a factory, employers squeeze surveilled workers, hoping to maximize focus, efficiency, and profits.[2] Workplace surveillance has evolved from being physically surveilled in the office or factory to more insidious algorithmic monitoring.[3] Even within the confines of the workplace, these techniques overstep the bounds of employee's expectations of privacy. However, as the global COVID-19 pandemic took hold, employees, confined to their homes, faced a brave new panopticon: software capturing, judging, and misjudging their every move. This software allows employers to police employee communication, expression, productivity, and jeopardize workplace wellbeing.

To face the new work-at-home phenomenon, employers sought solutions to make employees feel watched within the comfort of their own homes. Employers in the tech, legal customer service, eCommerce, and finance industries required their workers to install software on their computers to keep track of keystrokes and website visitation. Some software took periodic snapshots, occasionally capturing everyday life: a worker absent-mindedly picking their nose, a child running through their home, or a partner attempting to have a candid conversation.[4] Employer interest in certain kinds of employee monitoring software increased by 600% although, many studies have shown that lack of employee trust and extensive surveillance can lead to lousy workplace morale and worse quality of work.[5] In the thick of the stay-at-home order, articles from various news sources began to pop up with titles like "Your Boss is Watching You," drawing attention to the kinds of techniques that employers were using inside

1. MICHEL FOUCAULT, DISCIPLINE AND PUNISH 202-03 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1997).

2. Graham Sewell & Barry Wilkinson, '*Someone to Watch Over Me': Surveillance, Discipline and the Just-In-Time Labour Process*, 26 SOCIO. 271 (1992).

3. Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know it. (And Amazon Has a Patent for it.)*, N.Y. TIMES (Feb. 1, 2018), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

4. Bobby Allyn, *Your Boss Is Watching You: Work-From-Home Boom Leads to More Surveillance*, NPR (May 13, 2020, 5:00 AM), https://www.npr.org/2020/05/13/854014403/your-boss-is-watching-you-work-from-home-boom-leads-to-more-surveillance.

5. Eric Chemi, *Worker Monitoring Tools See Surging Growth as Companies Adjust to Stay-At-Home Orders*, CNBC (May 13, 2020, 6:08 PM), https://www.cnbc.com/2020/05/13/employee-monitoring-tools-see-uptick-as-more-people-work-from-home.html.

employees' homes. [6] This new software not only affects employee trust and productivity; they also have broad social implications.

This intrusion into employees' homes due to the global pandemic brings up a massive ethical conundrum that the current law has yet to address. The home has long been considered the last stronghold for the reasonable expectation of privacy.[7] Employees in the private workforce can expect zero to minor amounts of privacy within the workplace due to a history of jurisprudence protecting employer property interests over employees' privacy rights. Additionally, employers have worked to destroy the reasonable expectation of privacy through technology agreements forcing employees to waive their right to privacy. With little privacy protection at work for private-sector employees, employees could still count on a reasonable expectation of privacy in their home life.[8] Although peering into employee homelives through a webcam or recording home activity through algorithmic management software may feel problematic to most observers, courts have yet to determine if this is an offensive and illegal intrusion.[9]

Surveillance has been a historical staple of the workplace. After the industrial revolution, a system of surveillance known as "Taylorism" became a popular way to increase efficiency in production by simplifying workers' tasks and making it easy to discipline workers who were not conforming.[10] However, despite its historical roots, private sector employee surveillance is minimally regulated by the common law and The National Labor Relations Act. As it begins to seep into the home and technology advances, judicial interpretation and legislation must address the issues that at-home surveillance creates more adequately.[11] In the following sections, I outline the history of surveillance and existing privacy protections within the workplace, explore new the kinds of technology used in the at-home sphere, address the problems that arise socially and legally as a result of this invasive software, and apply a comparative approach to proscribe a legal solution to the socio-political problem that increased surveillance has created. In Section I, I argue that historically, surveillance in the workplace has been a tool for power solidified under a legal tradition that emphasizes an employer's property interest over a worker's privacy rights. In Section II, I address the new technology used in the at-home workplace and the many social and political implications. Additionally, I argue that the current legal framework to analyze privacy fails to address these issues. Finally, in section

6. *Id.*

7. Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83 (2008).

8. *Id.* at 83-84.

9. *Id.* at 84.

10. Ifeoma Ajunwa, Kate Crawford & Jason Schultz, *Limitless Worker Surveillance*, 105 CAL L. REV. 735, 771 (2017).

11. *Id.* at 736.

III, I argue that there is a way to balance employer interests in surveillance and employee interests for privacy by reimagining the legal framework through a comparative approach.

II. HISTORY OF SURVEILLANCE AND EXISTING PRIVACY PROTECTIONS

A. A BRIEF HISTORY OF SURVEILLANCE IN THE WORKPLACE AND HOW IT IS EXECUTED

Surveillance techniques in the workplace began during the industrial revolution on the factory floor.[12] In order to max out productivity and efficiency, employers sought techniques to discipline workers.[13] Scientific management became an answer to regularizing and increasing worker productivity.[14] As a result, factory owners began to pay consultants large amounts of money to establish new workplace regimes that maximized profit and relied heavily on surveillance.[15]

Some observers have compared the new factories and oversight techniques that emerged from this era to that of a prison.[16] These oversight techniques closely resembled the architectural phenomenon coined "the Panopticon," designed for prisons by Jeremy Bentham.[17] This structure is identified by its large central tower surrounded by inward-facing prison cells.[18] In his analysis of the tower, Bentham describes the tower as follows:

> The Inspection-Tower: comprehending on one story the lowermost Inspection- Gallery; with the inclosed Inspector's Lodge; in another, the middlemost Inspection-Gallery, in which is enclosed the lowermost Chapel-Galler, in which is enclosed the lowermost chapel-Gallery, and within that again the Area of the Chapel; on a third; the uppermost Chapel-Galler. The Cellular mass, together with the Inspection Tower inclosed within it, compose the characteristic part of the building: the projecting Front forms an accidental and inessential appendage. [19]

Most importantly, Bentham's structure allowed all of those residing in the tower to gaze into all of the cells at one time.[20] According to Michel Foucault, the effects of the panopticon created a "permanent visibility that

12. Sewell & Wilkinson, *supra* note 2.

13. *Id.*

14. Ivan Manokha, *New Means of Workplace Surveillance: From the Gaze of the Supervisor to the Digitalization of Employees*, 70 MONTHLY REV. 9, 28-29 (2019).

15. Sewell & Wilkinson, *supra* note 2, at 272.

16. *Id.*

17. JEREMY BENTHAM, *Part 1: Containing Further Particulars and Alterations Relative to the Plan of Construction Originally Proposed; Principally Adapted to the Purpose of a Panopticon Penitentiary-House in* PANOPTICON: POSTSCRIPT (London, Printed for T. Payne 1791).

18. *Id.* at 1-7.

19. *Id.* at 5-6.

20. *Id.* at 13-20.

assures the automatic function of power."[21] In effect, these structures created an internalized feeling of surveillance. They manifested the disciplinary dynamic that instilled a feeling of subordination—of being constantly monitored, within the prisoner, without them having an uneasiness of being constantly monitored.[22]

Meanwhile, another Utilitarian, Fredrick Winslow Taylor, was gaining traction through reforming the factory system and its efficiency.[23] By the time of his death in 1915, Taylor was known as the creator of scientific management.[24] From an industrial background, Taylor became fascinated with making workers move quickly and efficiently as if they were machines.[25] He believed that all work could be produced at the same pace if workers followed the proper procedures.[26] Taylor would first break down a job into its parts and then time each part with a stopwatch to determine the rate at which jobs were most efficient.[27] Scientific management refers to the belief that the length of time it should take for each person to complete a job could be determined.[28] However, much scientific management relied on arbitrary assumptions about time.[29] To Taylor, the most efficient form of shop management would allow the employer to have total control of the job and enforce a standard work pace.[30] In order to incentivize workers to produce at that rate, Taylor proposed a system of incentivized wages.[31] Taylor's system called the piece rate system paid employees by the piece instead of by the hour.[32] Job times were to be determined by Taylor's time study, and workers who took longer were paid at a meager rate.[33] A certain amount of monitoring became required to maintain this system.

This feeling of uneasiness or of constantly being monitored became essential in the power dynamics produced through structures of the traditional factory and, later, the office space. In the factory, Taylor's production regime meant to increase total output relied on a "total surveillance" system to ensure the maximization of profits.[34] This system of total surveillance touted an ideology that an unsupervised worker was an

21. FOUCAULT, *supra* note 1, at 201-02.
22. Sewell & Wilkinson, *supra* note 2, at 274.
23. HUGH G. J. AITKEN, SCIENTIFIC MANAGEMENT IN ACTION: TAYLORISM AT WATERTOWN ARSENAL, 1908 – 1915, 13 (Princeton University Press 1985) (1960).
24. *Id.* at 14.
25. *Id.* at 19.
26. *Id.* at 21.
27. *Id.* at 22.
28. *Id.*
29. *Id.* at 24.
30. *Id.* at 41.
31. *Id.* at 35.
32. *Id.*
33. *Id.* at 41.
34. *Id.* at 27.

inefficient worker.[35] Information was transferred faster under this surveillance regime, and an immediate reprimand for perceived inefficiency occurred.[36] These profit-maximizing regimes called just-in-time and total quality control allowed the factory floor to be more streamlined and grouped people by similar functions.[37] These regimes increased visibility on the factory floor and made the surveillance of workers easier.[38] Information traveled quickly, and supervisors were able to discipline quickly as a result.[39]

In the early 20th century Henry Ford took surveillance in his factories to another level.[40] The idea that society could be structured along the lines of a factory became Fordism.[41] Not only did he saunter around the factory checking for worker speed and efficiency, but he also spied on workers in their private lives.[42] He believed that challenges in his employees' personal lives, or rather lack of morality, would lead to less productivity in the workplace.[43] Ford began a sociological department charged with interviewing workers about their lives and work at his factory.[44] Questions often centered around marital status and finances to determine if they were worthy of working.[45] As a result, he became increasingly interested in his employee's health and hygiene.[46] He began to condition higher wages on living healthy and moral lifestyles.[47] Ford's surveillance of workers' personal lives became essential to his experiment in structuring society like a factory floor.

Similar to Taylorism and Fordism, a phenomenon of surveillance developed in office spaces.[48] Like the factory, "the office" is a building that houses another specific form of labor organization.[49] Office spaces house non-manual, mental, indirect work.[50] In the 1960s, due to the change in technology, growth of the workforce, and rise in a service-based economy, offices became the predominant organizational form for labor.[51] Offices

35. *See* Manokha, *supra* note 14, at 29.
36. *Id.* at 35.
37. *Id.* at 28-29.
38. *Id.* at 19.
39. *Id.*
40. Ajunwa et al., *supra* note 10, at 741.
41. Ted Morgan, *Intrigue and Tyranny in Motor City*, N.Y. TIMES (July 13, 1986), https://www.nytimes.com/1986/07/13/books/intrigue-and-tyranny-in-motor-city.html.
42. *Id.*
43. *Id.*
44. *Id.*
45. *Id.*
46. Manokha, *supra* note 14, at 29.
47. *Id.*
48. Michelle Murphy, *Toxicity in the Details: The History of the Women's Office Worker Movement and Occupational Health in the Late-Capitalist Office*, 41 LAB. HIST. 189, 193-94 (2000).
49. Christopher Baldry, *The Social Construction of Office Space*, 136 INT'L LAB. REV. 365 (1997).
50. *Id.*
51. *Id.*

utilized open floor plans with cubicles[52] instead of the usual organization by factory rank.

Information flowed freely because workers kept track of one another within their group.[53] As a result, this increased efficiency of information flow led to a new popular office layout that allowed for easy surveillance and the feeling of being constantly monitored.[54] The typical office stereotype we recognize today resembles a factory floor under Fordism and Taylorism.

As technology has shifted, surveillance techniques by employers in the private sector have become even more invasive. Today, surveillance in the workplace can take several forms: use of personal data, biometrics, and covert surveillance used to monitor employee productivity and lifestyle choices.[55] The use of personal data refers to electronic employee records for actual and prospective employees.[56] The use of biometric data refers to fingerprinting, alcohol and drug testing, and general health data.[57] Companies like Microsoft and Amazon have filed patents for employee well-being and monitoring software.[58] Similar to Ford's team of sociologists, the goal of this software is to track employee lifestyle choices to relate them back to their work and productivity. Amazon, for example, requires warehouse employees to wear a device that alerts them of how much time they have to meet a target and the shortest route.[59]

More and more corporate offices utilize surveillance cameras and software monitoring to analyze employee emails and social media presence.[60] Using Artificial Intelligence, companies monitor employees' internet use, keystrokes, and track employee emails.[61] Employer-provided computers are free-game for constant monitoring during work hours, and employer-provided cell phones allow employers to track an employees' location through G.P.S.[62] These programs allow for employee location tracking both on and off the job.

These forms of covert surveillance have created a billion-dollar industry for software used to monitor employees' electronic devices to increase productivity specifically.[63] Advertisements pepper the internet for software

52. *Id.*
53. *Id.*
54. *Id.*
55. Kirstie Ball, *Workplace Surveillance: An Overview,* 51 LAB. HIST. 87 (2010).
56. *Id.*
57. *Id.*
58. *Id.*; Ceylan Yeginsu, *If Workers Slack Off, the Wristband Will Know it. (And Amazon Has a Patent for it.),* N.Y. TIMES (Feb. 1, 2018), https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.
59. Manokha, *supra* note 14, at 31.
60. *Id.* at 30.
61. Ajunwa et al., *supra* note 10, at 743.
62. *Id.* at 743, 750.
63. Manokha, *supra* note 14, at 30.

solutions that allow employers to track their employees' productivity.[64] Some firms have developed devices that track employee social dynamics with hidden microphones, location sensors, and accelerometers on their I.D. badges.[65] Companies state that this tracking aims to analyze employee social interactions and link them to performance.[66] In studies, the firm found that workers that took breaks in tightly knit groups had more productivity and were more likely to stay.[67] Like Ford and Taylor, companies are essentially reducing employees to experiments on productivity without going through the scientific process of proving causation.

Algorithms drive gig work and work that requires online platforms and relies exclusively on worker surveillance to maximize profits.[68] Instead of a supervisor standing over an employee's shoulder, algorithms and rating systems determine the earnings gig workers receive.[69] Ford's incredibly invasive surveillance technique has been remediated into new forms of technology. These surveillance technologies are rampant within the gig workplace today.

Employees bring these same techniques home as the living room has replaced the office. The panopticon, once an architectural structure created for a prison environment, has become a constant in the lives of everyday workers. As technology has rapidly changed the culture of surveillance in the workplace, the law has done little to stop employers from going too far. In the next section, I will examine the existing privacy laws for employees within the confines of the workplace.

A. EXISTING PRIVACY LAWS FOR EMPLOYEES WITHIN THE WORKPLACE

Although there is a substantial history of surveillance in the workplace, U.S. privacy laws have done little to curb the extensive use of these invasive techniques. Courts have often found that employers have legitimate reasons for monitoring employees in the workplace.[70] These reasons are derived from the employer's property rights and usually manifest themselves through the

64. HUBSTAFF, https://hubstaff.com/?utm_campaign=Hubstaff%20Signup&utm_source=ppc&utm_medium=Google%20Ads&utm_term=branded_search&utm_content=Channels&gclid=CjwKCAjwwsmLBhACEiwANq-tXCkPUSlIJJVTGv3-yvw_OhOliSO-7_6bCfg9GRXCzClD9c2PaHwPaxoCU0gQAvD_BwE.

65. *Id.*

66. Ajunwa et al., *supra* note 10, at 743.

67. *The Rise of Workplace Spying*, THE WEEK (July 5, 2015), https://theweek.com/articles/564263/rise-workplace-spying.

68. Gheorghe H. Popescu et al., *Algorithmic Labor in the Platform Economy: Digital Infrastructures, Job Quality, and Workplace Surveillance*, 13 ECON., MGNT. AND FIN. MKTS. 74, 79 (2018), https://www.proquest.com/docview/2116360195?accountid=33497.

69. *Id.* at 78.

70. *See* Sprague, *supra* note 7, at 114-17.

security of trade secrets and protection of valuable property.[71] While employers say they need the power to surveil to monitor and increase worker productivity, many employers also monitor employee behavior to ensure safe work environments. For example, employers may ensure that the websites that their employees visit are not pornographic or overtly racist.

Because of these rationales, protections for employee privacy rights against surveillance in the workplace are limited for internet surveillance. In the public sphere, employees are extended the right to privacy through the 4th amendment.[72] Private employees only enjoy some protection from state constitutions and common law. While concerned about the adverse effects of coercive surveillance on union elections, the Federally enacted National Labor Relations Act (NLRA) additionally includes some protection against surveillance.

Privacy is driven in U.S. jurisprudence mainly by the concept that a person may have a reasonable expectation of privacy in a place society is willing to recognize as private and that a person subjectively thought was private.[73] The reasonable expectation of privacy stems from the 4th amendment's prohibition against unreasonable searches and seizures.[74] However, this expectation of privacy is often not transferred to the workplace because of the employer's right to property. Even employees' little privacy expectations can be eliminated through a notice in employee handbooks and software agreements.[75] Employers often alert their employees of monitoring, putting them on notice that they do not have a reasonable expectation of privacy while on their computers or in the office space. Notice essentially destroys any assumption that an employee would have deemed a space private because they were aware of the employer's monitoring. Therefore, the notice would eliminate an employee's subjective and objective expectation of privacy.

Public employees have their right to privacy protected by the 4th amendment's prohibition against unreasonable searches and seizures.[76] For example, in the *City of Ontario v. Quon*, an officer was provided a pager from the police department.[77] Many of the officers had gone over their plans, and as a result, the police department had determined that an audit would be necessary to determine if they needed to expand the plan or enter into disciplinary action.[78] The department found that only 13% of the messages

71. *Id.* at 111-12.

72. City of Ontario v. Quon, 560 U.S. 746(2010).

73. Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979 (2011).

74. U.S. CONST. amend. IV.

75. Determann, *supra* note 73, at 981.

76. *Id.*

77. *Id.*

78. *Id.*

were work-related due to the audit.[79] Mr. Quon sued under the 4th amendment and argued that the search violated his reasonable expectation of privacy.[80]

In order to analyze Mr. Quon's reasonable expectation of privacy, courts look to social norms and the actual workplace policies in place.[81] The police department had a policy noting that the employer would monitor all communications but did not mention pager messages.[82] The Court looked to whether the search was justified at its inception and reasonable in its scope.[83] The Court found the search to have been reasonable because the audit only examined messages within the two-month window of overages and did not look at any off-duty text messages.[84] Thus, even when protections for employee privacy exist in the public sector, courts give employers broad discretion in determining what kind of search is reasonable. Additionally, these decisions have incentivized comprehensive workplace technology policies to escape liability.

Unlike public employees, private employees are not protected by the 4th amendment. Private employees rely on common law rights to privacy, state constitutions, and statutes. However, these protections are limited. For example, only Delaware and Connecticut have statutes that require employers to inform their employees that they are electronically tracking them.[85] The common law rights to privacy include protection against 1) intrusion upon seclusion; 2) public disclosure of embarrassing private facts; 3) publicity which places a person in a false light, and 4) commercial appropriation of a person's name or likeness.[86] Like public sector employees, private employees need to demonstrate that they have a reasonable expectation of privacy.[87] Courts give tremendous discretion to employers while analyzing the Right to Privacy Tort regarding workplace surveillance. Employers can quickly destroy someone's reasonable expectation of privacy through employee handbooks and other forms of notice and consent forms.[88]

Stengart v. Loving Care gives some guidance for how Courts analyze the right of privacy tort regarding workplace technology. In *Stengart*, Ms. Stengart was given a personal computer by her employer to work flexibly.[89] Unbeknownst to her, the personal computer had software installed to capture

79. *Id.*
80. *Id.*
81. *Id.*
82. *Id.* at 758.
83. *Id.*
84. *Id.*
85. Ajunwa et al., *supra* note 10, at 743.
86. Determann, *supra* note 73.
87. *Id.* at 991.
88. *Id.* at 992.
89. Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 990 (2010).

an image of what was on her hard drive at intervals throughout the day.[90] Ms. Stengart filed a complaint about her employer when she took the laptop home to review her emails.[91] As she logged into her password-protected personal email to view emails from her attorney, the software took a snapshot.[92] This snapshot revealed confidential information shared with her attorney that the employer now possessed.[93] As a result, Ms. Stengart sued for her right to privacy.

Under the right to privacy tort, an employee has a reasonable expectation of privacy of a physical, electronic work location if: the employer has provided express notice that the location is private, the employer has acted in a manner that treats the location as private for employees, the type of location is customarily treated as private for employees, and the employee has made reasonable efforts to keep the location private. In the case of Ms. Stengart, the Court determined that she did have a reasonable expectation of privacy.[94] The Court reasoned that because Ms. Stengart's email was password-protected, that evidenced that she had made reasonable efforts to keep the location private.[95] Her conversations with her lawyer are treated customarily as private under attorney-client privilege.[96] As a result, the Court held that Ms. Stengart had a reasonable expectation of privacy to the communication with her lawyer.

The California Constitution sets a standard similar to the tort of intrusion. The California Constitution states, "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein."[97] To determine whether an employer has intruded, the Court analyzes the following elements of the tort of intrusion: 1) the defendant must intentionally intrude into a place, conversation, or matter to which the plaintiff has a reasonable expectation of privacy and 2) the intrusion must occur in a manner highly offensive to a reasonable person.[98] This standard makes it incredibly difficult to determine what kinds of highly offensive intrusions. The idea that our employers are sifting through our emails may be offensive to our commonsense notions of privacy. However, much of the case law is outdated. With cases that deal with instances of video surveillance in changing rooms and instances of strip-searching, it is hard to know where email surveillance fits concerning

90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*
96. *Id.*
97. CAL. CONST. art. I, § 12.
98. Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 211 (2009).

what is offensive.[99] As a result, there is not much line drawn about how offensive the intrusion needs to be.

The California Supreme Court attempts to tease out an offensive intrusion in *Hillsides v. Hernandez*.[100] In *Hillsides*, the plaintiffs were two clerical workers working for neglected and abused children at a nonprofit residential facility. [101] The plaintiffs sued the facility director, alleging that he violated their rights to privacy under the California Constitution by secretly installing a video camera in their office.[102] The manager installed a camera after the I.T. manager had found records of pornography being watched from one of the computers late at night in the office.[103] The manager did not alert the employees of the video camera, although the camera was used at night.[104] The employees argued that they often used the office to change and assumed it was a private space.[105]

The California Supreme Court came to different conclusions regarding each element of the tort of intrusion.[106] Regarding the first element, the Court held that there could be a reasonable expectation of privacy. The Court concluded that there is a reasonable expectation of privacy behind closed doors in an office and that it was a reasonable assumption that their employer would not install a video camera without their knowledge or consent.[107] In articulating the rule, the Court stated, "[o]ur analysis starts from the premise that, while privacy expectations may be significantly diminished in the workplace, they are not lacking altogether."[108] The Court held differently for whether the intrusion itself was highly offensive.[109] The Court emphasized the importance of the scope of the surveillance. The Court held that the surveillance intrusion was not offensive because the camera was only turned on at night and did not capture any surveillance of the two employees.[110] The Court stated:

> In adopting this refined approach, Sanders highlighted various factors which, either singly or in combination, affect societal expectations of privacy. One

99. *Compare* Bodewig v. Kmart, Inc., 635 P.2d 657, 661 (Or. Ct. App. 1981) (contending the humiliation of an employee being forcibly strip-searched by her employer in a changing room due to the unreasonable demands of a customer exceeded the bounds of social toleration), *with* Hernandez, 211 P.3d at 1066-70 (rejecting the claim that the intrusion of employer video surveillance limited in scope was highly offensive to constitute a privacy violation even though there was potential for that surveillance to include an employee changing clothes).

100. Hernandez, 211 P.3d at 1066.

101. *Id.* at 1067.

102. *Id.*

103. *Id.* at 1068-69.

104. *Id.* at 1069.

105. *Id.* at 1070.

106. *Id.* at 1074-80.

107. *Id.* at 1074.

108. *Id.*

109. *Id.* at 1078.

110. *Id.* at 1079.

> factor was the identity of the intruders…. Also relevant in Sanders, was the nature of the intrusion, meaning, both the extent to which the subject interaction could be 'seen and overheard' and the 'means of intrusion.'[111]

The Court additionally gave leeway to the employer due to the solid countervailing interest concerning the wholesome environment of the children's home.[112]

As demonstrated in *Hernandez v. Hillsides*, California does recognize a reasonable expectation of privacy in the workplace. However, courts have granted broad discretion to employers regarding scope. This case illuminates where an employee could have a reasonable expectation of privacy (behind closed doors in an office); however, it still demonstrates another hurdle for employees to demonstrate that the employer's conduct was offensive. Additionally, although intuitively, one could translate these protections to the workplace at home because it is a private space, workers are often asked to consent to surveillance. Through notice and consent, employers can destroy an employee's reasonable expectation of privacy in specific spaces in the office. One of the essential aspects of *Hernandez v. Hillsides* is that the employer did not inform the two employees that they were being surveilled.[113] Employees often sign technology agreements presented by their employers that confirm that they can no longer view a space as having a reasonable expectation of privacy. It has become challenging for employees even to reach the offensive prong because these agreements stamp out any reasonable expectation of privacy.

Federal law additionally offers minimal protections against surveillance in the workplace. Section (7) of the NLRA states that employees "have the right to self-organize, to form, join, or assist labor organizations, to bargain collectively through representation of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection."[114] Section (8)(a)(1) of the NLRA adds that it is an unfair labor practice "to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7."[115] Under section (8)(a)(1), excessive surveillance can be viewed as an unfair labor practice.

During an election it can be seen as a natural reaction of the employer to try and gain information about Union organizers and supporters.[116] However, the Board has traditionally found that employers rarely justify posing information about the employee's union activity and the union's

111. *Id.* at 1074.
112. *Id.* at 1081.
113. *Id.* at 1069.
114. 29 U.S.C. § 157.
115. 29 U.S.C. § 158(a)(1)
116. ROBERT E. WILLIAMS ET AL., NLRB REGULATION OF ELECTION CONDUCT: A STUDY OF THE NATIONAL LABOR RELATIONS BOARD'S POLICIES AND STANDARDS FOR SETTING ASIDE REPRESENTATION ELECTIONS BASED ON POSTELECTION OBJECTIONS 167 (1974).

campaign.[117] The Board's decisions often reflect an absolute right to privacy when an employee is exercising their rights under Section 7.[118] When it comes to surveillance of employees while exercising their rights under the Act, it is usually deemed unlawful.[119] Additionally, during an election period, surveillance can lead to an election set aside by the Board.[120] The Board sees surveillance as detrimental to workers attempting to exercise their right to organize without the threat of reprisal from their employer.[121]

Surveillance in many of these cases involves management surveilling workers or creating the impression of surveillance at union meetings or elsewhere through the use of photographs, video surveillance, and informants.[122] For surveillance to be lawful, it needs to be reasonably justified for a legitimate purpose.[123] The Board will scrutinize an employer's purpose for surveilling employees during protected activities.[124] The Board heavily scrutinizes surveillance because of the psychological effects on employees not knowing what kind of information their employer has gathered on them.[125] Photographing employees during campaigning is held to a higher standard of scrutiny due to their propensity to intimidate.[126] Making employees perceive that they are being surveilled can also be seen as unlawful activity. Although not gathering the information, it still is meant to make employees feel intimidated to exercise their rights.[127]

There are some futile constraints on the employers' ability to destroy the right to privacy through alleged consent.[128] For example, as technology advances, employers are beginning to be held to a higher standard of specificity in their notice and consent within their technology agreements.[129] However, this is often alleviated by the creation of attentive in-house legal counsel. Employers' legal departments are often incredibly meticulous and write particularized technology agreements. These tactics beg the question of whether an employee is genuinely consenting. Additionally, the assumption that intense competition in the at-will job market will prevent employees from choosing to work for employers with invasive surveillance seems to only apply to workers with a large amount of bargaining power.

117. *Id.*
118. *Id.*
119. *Id.* at 188.
120. *Id.* at 189.
121. *Id.*
122. *Id.*
123. *Id.* at 191.
124. *Id.*
125. *Id.* at 189.
126. *Id.* at 191.
127. *Id.*
128. Determann, *supra* note 73, at 994.
129. *Id.*

Some states do have certain statutory privacy protections for employees. Connecticut and Delaware both have statutes requiring employers to notify employees that they monitor their communications. [130] Additionally, several states require consent from all parties to record conversations.[131] California's statute, however, has an exemption to parties that could reasonably expect that their conversations are overheard.[132] Because there is generally no reasonable expectation of privacy in the workplace and a conversation can likely be overheard, it is unlikely that the statute will apply.

Legally, minimal stands in the way of an employer's attempt to gain information about their employee's performance, social lives, and private conversations. Although most public employees receive protections against unreasonable searches and seizures, the Court still grants broad discretion to the employer's interests. Private employees receive even fewer protections from the peering eye of their employers. With protections only reserved by common law for the most egregious privacy violations, employers are relatively free to track employee emails and private communications. Only employees who have strong bargaining power have the option of refusing to tolerate an employer's surveillance. As a result, the judicial system has barely even scratched the surface in providing privacy protections to employees.

III. HOW NEW TECHNOLOGY HAS CREATED POTENTIAL PROBLEMS FOR THOSE WORKING FROM HOME

A. AT HOME SURVEILLANCE TECHNIQUES

As surveillance techniques have become more and more invasive within the workplace, employees have been forced to bring them home as offices shut their doors due to the COVID-19 pandemic. In March of 2020, the world drew to a screeching halt. The novel Coronavirus spread rapidly across the United States, and businesses closed their doors as the news predicted that the shutdown would be temporary. The world soon found out that it was not. Employers began extensive work from home programs while the government mandated that non-essential workers stay home. COVID-19 proved that it was here to stay, and employers began to grapple with anxieties about employee productivity. Employers began to employ the same surveillance techniques for at-home assignments that were used in the workplace to hold employees accountable

130. *Id.*
131. *Id.*
132. Cal. Penal Code § 632(c).

Stories all over the internet summarized ways in which "Your Boss is Watching." Surveillance became a staple across the labor market at home that affected both low- and high-income workers. In an article for the *Washington Post*, an attorney, Kerrie, describes her experience with facial recognition software installed by her employer.[133] When Kerrie was hired in the spring for a popular legal job, she was sent a company issue laptop where she believed she would review legal files from the comfort of her home.[134] However, when she received her laptop, she soon realized that she would need to comply with its facial recognition software as a term of her employment.[135] Through the camera on the computer, the software would monitor her every move.[136] She described how simply shifting in her chair or looking away would mean that she had to scan her face back in.[137] It became so stressful that she ended her employment with this particular company.[138]

The stress associated with the feeling of being surveilled became a reality for many Americans— if not through the use of facial recognition software, then through other forms of productivity tracking software. In An interview for NPR in May of 2020, a worker described her experience as an eCommerce worker. Two weeks into working from home, her company required her to install software from Hubstaff on her personal computer.[139] This software tracked mouse movements, keyboard strokes and recorded webpages visited.[140] Additionally, employees were required to download an application on their smartphones called TSheets that would allow their employer to track their location.[141] One of the interviewees describes the stress the software put on employees, "I just feel like crap. I feel like I'm not trusted. I feel ashamed of myself. My co-workers were really, really upset. But everyone was too afraid to say anything."[142]

The Hubstaff website paints a different picture. The main page has a glossy slogan that reads, " spend less time tracking and more time growing."[143] Hubstaff's features include time tracking, proof of work,

133. Danielle Abril & Drew Harwell, *Keystroke Tracking, Screenshots, and Facial Recognition: The Boss May Be Watching Long After the Pandemic Ends*, WASH. POST (Sept. 24, 2021, 7:00 AM), https://www.washingtonpost.com/technology/2021/09/24/remote-work-from-home-surveillance/.

134. *Id.*

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

139. Allyn, *supra* note 4.

140. *Id.*

141. *Id.*

142. *Id.*

143. HUBSTAFF, https://hubstaff.com/?utm_campaign=Hubstaff%20Signup&utm_source=ppc&utm_medium=Google%20Ads&utm_term=branded_search&utm_content=Channels&gclid=Cj0KCQjww4OMBhCUARIsAILn

reporting, metrics, and automated payroll.[144] The product installed on the management's screen includes all the employee's performance metrics.[145] This view allows employers to see weekly activity, daily activity, hours worked during the week, projects, and screenshots of employees' recent activity on their computers.[146]

In an article for the *New York Times*, Adam Satariano tests employee monitoring software that more and more employers require of employees.[147] Satariano explains that Hubstaff. has been a popular software program used for years by Wall Street firms, primarily for security purposes.[148] As he monitored himself through the software, Satariano noticed how his behavior quickly changed. He became obsessed with his productivity score.[149] He stated:

> "Each day I logged in early because it was keeping a running clock of my activity. Knowing my online actions could be reviewed I did not spend (as much) time reading about sports and rarely opened messaging apps on my laptop, nervous about a screenshot catching a private exchange. But my activity scores stayed stubbornly low, usually form 30 percent to 45 percent."[150]

The vast array of personal information gathered from his computer led to many questions of discretion given to managers and potential for abuse.[151] Managers were able to view the screenshots the software took, and the employees frequently visited websites through the manager portal of the software.[152] This portal would allow managers to observe everything occurring on the laptops of the employees they supervised.[153] The program's ability to grab a screenshot on the off chance an employee forgot to log out allows personal conversations to become vulnerable to fellow employees. Hubstaff requires employees to log in and log out at the end of the day.[154] It continuously works throughout this timeframe.[155] Satariano explains:

> "The moment I no longer wanted to be monitored came on April 23 at 11:30 am., when Hubstaff caught me doing an internet exercise class. By the time I

dv6w2M7EfKvmOmXhNDN4vpyKftyOUd_QWB1_OJpv53DfcYi232AGzCIaAmCNEALw_wcB (last visited Feb. 13, 2022).

144. *Id.*
145. *Id.*
146. *Id.*
147. Adam Satariano, *How My Boss Monitors Me While I Work from Home*, N.Y. TIMES (May 6, 2020), https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html.
148. *Id.*
149. *Id.*
150. *Id.*
151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. *Id.*

> realized I had not logged out, it had snapped a screenshot of the trainer setting up to teach the class in her living room."[156]

Although employers might not be purposefully seeking this information, an employee's simple mistake might lead to accidentally sharing sensitive information with the employer or a nosy manager.

B. POTENTIAL PROBLEMS

The at-home employee monitoring industry has seen extreme growth. During the pandemic, at-home surveillance has risen to 60% of employers requiring employees to bring surveillance home with them.[157] That number is expected to rise within the following year.[158] Hubgroup's stock prices have risen 51.18% in the last year, reflecting this new work -from -home dynamic.[159] Additionally, companies like Prodoscore (a similar employee monitoring software) have seen interest from prospective customers climbing 600%.[160] According to Google Trends, people are searching for "employee monitoring" more and more.[161] Some articles even rank monitoring software, helping employers find the right fit for their companies.[162] For example, the top choice Teramind's review reads:

> Teramind's comprehensive tracking functionality can capture any user activity. These can range from screen recordings, like views of employee P.C.s tracking emails and keystrokes to Zoom sessions, all of which earns it our Editors' choice pick for employee monitoring.[163]

With the growth of at-home surveillance, the software is predicted to become more sophisticated and invasive.[164] So much so that it will be able to track how much employees contribute during video conferencing and whether they collaborate well.[165]

The growth of this software use does not just raise privacy concerns. These programs also manifest biases in the same ways that humans do. Facial recognition software is created within social contexts that allow these forms

156. *Id.*
157. Abril & Harwell, *supra* note 133.
158. *Id.*
159. *Id.*
160. Chemi, *supra* note 5.
161. *Id.*
162. Neil McAllister, *The Best Employee Monitoring Software for 2022*, PC MAG (Jan. 20, 2022) https://www.pcmag.com/picks/the-best-employee-monitoring-software (PC Magazine reviewed different kinds of employee monitoring software like they do with other new tech products that reach the market. Teramind, like Hubstaff, is a comprehensive employee tracking software. It captures screen recordings, live views of employees' P.C.s, track emails, keystrokes, and zoom sessions. The ranking system seems to be based on the most invasive and extensive surveillance software).
163. *Id.*
164. Abril & Harwell, *supra* note 133.
165. *Id.*

to reflect gender, racial, and socioeconomic bias.[166] Although the tools used to monitor employees seems offensive to all. The growth of surveillance does not affect all workers evenly. Specific industries and identities are prone to increased surveillance.[167] The retail industry, which is made up of predominantly minority and female workers, is impacted by increased levels of surveillance.[168]

Because this software is so new, few protections for employee monitoring software exist. This software can only be actionable against the employer if it is considered highly offensive even when there is a presumably reasonable expectation of privacy within the home.[169] As articulated in *Hernandez v. Hillsides,* an offensive intrusion relies on many factors, and courts have ruled inconsistently on what is deemed to be offensive.[170] Often, what is offensive is guided by community norms and requires an objective analysis of the invasion.[171] The objective analysis includes factors such as 1) the likelihood of serious harm to the plaintiff and 2) the presence or absence of countervailing interests based on competing for social norms. [172] A countervailing interest could manifest itself as a legitimate public interest in exposing private information.[173] The legitimate public interest becomes a legitimate business interest in the private employer context.[174]

It should be challenging to argue that taking a screenshot of someone's personal computer or a photo of them every time they move away from their screen qualifies as a legitimate employer interest. However, the current legal framework recognizes a legitimate employer's interest in surveillance. Many employers argue that security and productivity reasons for surveillance outweigh the employee privacy interest. While security reasons can be somewhat legitimate, productivity is not necessarily maximized by the use of at-home surveillance, primarily, the kinds of invasive software used throughout the pandemic. In actuality, the surveillance techniques affect employees' cognitive functions due to stress and their morale by causing them to no longer trust the employer. This research brings into question

166. Luke Stark et al., "*I Don't Want Someone to Watch Me While I'm Working": Gendered Views of Facial Recognition Technology in Workplace Surveillance*. 71 J. OF THE ASS'N FOR INFO. SCI. & TECH. 1074, 1075 (2020), https://doi.org/10.1002/asi.24342 ("Training these systems on biased data gathered from unequal social contexts entrenches existing forms of discrimination, and the nature of the physiological classifications these systems produce inclines them towards the production of sexist and racist hierarchies.").

167. *Id.* at 1076.

168. *Id.*

169. Kyllo v. United States, 533 U.S. 27 (2001).

170. Hernandez, 47 Cal. 4th 272, at 211; Sprague, *supra* note 7, at 125.

171. *Id.*; Sprague, *supra* note 7, at 126.

172. *Id.;* Sprague, *supra* note 7, at 126; *see also* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 648 (Cal. 1994).

173. *Id.*

174. *Id.* at 642.

whether there is a legitimate reason for this kind of software that can outweigh an employee's interest in privacy.

The stress of having someone or something hovering over your shoulder has negative consequences for employees. In an article for the *Washington Post,* a worker describes the stress created by facial recognition software,

> It's just this constant, unnecessary, nerve-racking stress: you're trying to concentrate and in the back of your mind you know you're on camera the entire time. While you're reviewing a document, you don't know who is reviewing you.[175]

Additionally, the software changes the way people work. Instead of thinking about complex problems, employees are worried that they are not meeting their keystroke requirements.[176] Many of the stories in the news include workers who were either burnt out by the constant anxiety of the monitoring software or who felt that it was a step too far, leading to them quitting their jobs.[177] One employee noted:

> If you're idle for a few minutes, if you go to the bathroom or whatever, a pop-up will come up and it'll say, 'You have 60 seconds to start working again or we're going to pause your time.' I just feel like crap. I feel like I'm not trusted. I feel ashamed of myself.[178]

Trust in management is an essential aspect of the employee-employer relationship.[179] The concept of trust is essential to quality relationships, cooperation, and stability in the workplace.[180] Trust can be defined as confidence that one will not exploit the other's vulnerabilities.[181] Workers find it difficult to trust those who do not trust them[182] According to an Australian study published in 2015, Electronic Monitoring and Surveillance related negatively to worker trust.[183] The study noted:

> These findings support the notion that increasing the number of E.M.S. practices can induce a negative perception of management and subsequently affect the relationship between employees and management through undermining trust. By increasing the perceived trust barriers, employees may be less willing to engage with the management, creating less effective organizations.[184]

175. Abril & Harwell, *supra* note 133.
176. *See id*.
177. *See id.*
178. Allyn, *supra* note 4.
179. Peter J. Holland et al., *Electronic Monitoring and Surveillance in the Workplace: The Effects on Trust in Management, and the Moderating Role of Occupational Type*, 44 PERSONNEL REVIEW 161, 163 (2015), http://dx.doi.org/10.1108/PR-11-2013-0211.
180. *Id*.
181. *Id*.
182. *Id*. at 165–166.
183. *Id*. at 166.
184. *Id*. at 169.

Beyond the lack of trust created in the work environment, this kind of software often does not necessarily track productivity in the way that employers believe it does. Although it is easier to quantify productivity in psychical labor, for knowledge-based jobs (such as jobs requiring those to stay home), the same outcome can occur taking different routes.[185] Cognitive style and personality can determine the many routes that one may take to reach the outcome of a project.[186] These monitoring tools make assumptions about how a person can achieve maximum productivity when all working styles are unique.[187] By focusing on this one measure of productivity through time stamps and screen time, employees are commoditized and have the added stress of conforming to meet these objectives created by big data.[188]

There are many social implications for allowing this kind of surveillance to breach the reasonable expectation of privacy of the home. The lack of legal protections and flimsy definition of offensive intrusion has done little to help workers avoid the eye of their manager while their child plays in the background of their at-home office. The rapid growth of employee monitoring software has led to many employers requiring monitoring software to measure productivity, keystrokes, and the private iMessage you accidentally opened from your sister. Without regulation, employers have immense discretion to sort through screenshots taken of your laptop at certain hours of the day. Even though the home historically has been the last bastion of the reasonable expectation of privacy, courts have struggled to define an offensive intrusion and when an employer goes too far.

IV. INCREASING EMPLOYEE PRIVACY: PROPOSING A SOLUTION

Because the home and office are now linked, it is essential to have well-established privacy protections for employees against the intrusive surveillance of their employers. Employers would have information on employees' private lives within their homes without increased privacy protections for employees. This can have a detrimental effect on employee morale and productivity and give employers a tremendous amount of power over employees. Courts have long recognized the reasonable expectation of privacy within the home.[189] When employees do not have the same kind of bargaining power that an employer does, especially in a pandemic, it becomes impossible for employees to say no to intrusive surveillance software. Employers destroy the expectation of privacy by providing notice and consent where employees have no choice but to consent in order to keep

185. *Id*. at 165.
186. *Id.*
187. *Id.*
188. *Id.*
189. Sprague, *supra* note 7, at 100, 108.

their job. It would be possible to require a substantial business justification for offensive intrusion rather than a reasonable one to put employee's rights over the perceived ones of the employer.[190]

European countries have more robust protections for the data of employees. Although their privacy rights come from a statute rather than a Constitution, the E.U. requires all member states to have a provision restricting the gathering of personal data without consent.[191] The E.U. only allows employers to have the following exemptions: 1) a necessity to perform contractual obligations with the data subject, 2) individual's consent, and 3) a legal requirement to process personal data.[192] Member states of the E.U. require a high burden of proof for an employer to overcome these requirements.[193] Additionally, unlike in the U.S., where an employer can unilaterally destroy the reasonable expectation of privacy through notice, the employer must seek affirmative consent from the employee within the European Union.[194] Consent is considered only valid if the subject gave informed, voluntary, express, specific, and written consent to the use of their data. [195] It is difficult for the employer to gain voluntary consent in many member states because it is presumed that the consent is coerced in the employment relationship.[196] Additionally, an employee can revoke consent at any time, therefore rendering employee monitoring impractical for employers.[197]

While members of the European Union do not have the same rights for employers as in the United States, it is still important to note that unlike in the U.S., these countries recognize that the employer-employee relationship has a unique power dynamic. If the employer and employee relationship dynamic were deemed coercive, it would be difficult for an employee to consent to a technology agreement fully. The reasonable expectation of privacy would still exist without the ability of an employer to destroy the reasonable expectation of privacy unilaterally. This would allow each space to be evaluated through the lens of the subjective and objective expectation of privacy without the influence of the employer. Additionally, it would allow an employee to say no without consequence. As a result, employees have their privacy claims heard, and more jurisprudence will be formed regarding the use of invasive technological surveillance. Courts would then be able to analyze what kinds of surveillance reaches the level of offensive. Employees experiencing extensive surveillance from home would likely

190. *Id*. at 126.
191. Determann, *supra* note 73.
192. *Id*.
193. *Id*.
194. *Id*.
195. *Id*.
196. *Id*.
197. *Id*.

succeed in demonstrating a reasonable expectation of privacy within the home. Then, at least the Court will analyze whether taking a screenshot of someone's personal computer screen is offensive.

V. CONCLUSION

Employers have long since engaged in surveillance to gain power and control over employees.[198] Starting with scientific management at the end of the 19th century, Taylorism instituted a new regime focused on productivity over employee well-being.[199] Surveillance by supervisors was essential to allow the system to function. These systems were taken a step further with Fordism. Ford enlisted teams of sociologists to pry into the private lives of his employees to determine if they were fit to work in his factory.[200] When the economy shifted to a service-based economy in the mid 20th century, surveillance became a crucial aspect in the design and layout of the modern office space. Employers then began to monitor employees, aided by advancements in technology.[201] Soon, no email was safe, and private web browsing in the workplace became a thing of the past leading to a chilling effect of workplace expression.[202] Surveillance made its way to being a staple of the American workplace.

Very few privacy protections buffered employees from the intense scrutiny of employers.[203] Public and private employees needed to demonstrate that a reasonable expectation of privacy existed in the space they wished to deem private.[204] However, the reasonable expectation of privacy could easily be unilaterally destroyed by employers through notice and consent agreements signed by employees.[205] The uniqueness of the power dynamic between employer and employee makes it incredibly difficult for employees to say no to preserve their employment.[206] As a result, employee surveillance saw incredible demand and growth.

The COVID-19 pandemic forced the world to come to a complete stop and employees that were not deemed essential into the home. Employers worried about worker productivity as employees were no longer under the watchful eye of coworkers or management. They began to institute new surveillance techniques that were even more oppressive than those used in the workplace.[207] Employees were forced to sign technology consent

198. Ajunwa et al., *supra* note 10, at 743.
199. *Id*. at 771.
200. *Id*. at 741 -42.
201. *Id*. at 743.
202. *Id*.
203. Sprague, *supra* note 7, at 113.
204. *Id*.
205. *Id*. at 132.
206. *Id*. at 113.
207. Allyn, *supra* note 4.

agreements and install software on their computers that tracked their bathroom breaks, keystrokes, and tasks completed.[208] Through the watchful eye of employee management software, employers would have a front-row seat to their employees' private homelives.[209] Through the software, employers could see screenshots of private messages, children running in the background of the laptop camera, or overhear a private conversation with a partner.[210] The home has long been considered a safe haven for privacy. However, employers have been operating unchecked by a legal system that values employer property interests over employee privacy interests. This invasive technology has problematic social implications such as chilling speech and adverse effects on employee well-being. Employees reported increased stress and changed views of their employer during an already stressful time. Without privacy reform, employees will be forced to bring the panopticon home for the foreseeable future.

208. *Id.*
209. *Id.*
210. *Id.*

***