Santa Clara University
School of Law

Santa Clara Law Review

Volume 57 | Number 1 Article 8

8-17-2017

#Privatesphere: Can Privacy Laws Adequately Protect Employees Amidst the Complexities of the Modern Employment Relationship?

Emily J. Tewes

#PRIVATESPHERE: CAN PRIVACY LAW ADEQUATELY PROTECT EMPLOYEES AMIDST THE COMPLEXITIES OF THE MODERN EMPLOYMENT RELATIONSHIP?

Emily J. Tewes*

* Symposium Editor, Santa Clara Law Review, Vol. 57; J.D. Candidate, Santa Clara University School of Law, 2017; B.A. Politics, University of California, Santa Cruz, 2010. Thank you to my fiancé, family and friends for your love and throughout law school. Special thank you to the Vol. 57 Editorial Board for their skillful work on this Comment.

INTRODUCTION

Modern employment trends threaten to jeopardize what little privacy protections American workers have.[1] Trends like private amenities on corporate campuses, using a single device for both work and personal purposes, social media usage, and the "24/7 workplace" provide more potential than ever before for privacy invasions while simultaneously denying employees the opportunity to obtain meaningful remedies for those invasions.

The crux of the failure to adequately protect employee privacy lies in the structure of the legal standard itself. Traditional privacy laws are deeply rooted in a flawed conceptual underpinning–the notion that legally protectable privacy in the employment relationship exists in a neatly discernable "private sphere."[2] This concept undermines the effectiveness of the legal tests[3] to expand or even maintain privacy protections in employment.[4]

First, this comment will identify the problem that modern employment trends collapse distinctions between private and work

1. *See* Ronald P. Angerer II, *Moving Beyond A Brick and Mortar Understanding of State Action: The Case for A More Majestic State Action Doctrine to Protect Employee Privacy in the Workplace*, 4 CHARLOTTE L. REV. 1, 4 (2013) (describing the current state of American employment law as "woefully inadequate in promoting and protecting employee privacy at the workplace.").

2. *See generally* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 555 (2006).

3. A subjective-objective determination of the "reasonableness" of an employee's privacy expectation operates as a threshold consideration to establishing privacy right in the employment relationship. *See generally* Katz v. United States, 389 U.S. 347 (1967).

4. Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 291 (2011) (advocating for a recognition of actual employment monitoring policies because "[s]uch recognition must lead to a rebalancing of current legal provisions to reflect the realities of the twenty-first-century workplace.").

spheres rendering the legal standards to determine privacy invasions at work futile. Second, this comment will explore the modern technologies and work structures that complicate the effective application of traditional privacy tests. Third, this comment will trace the historical development of privacy law and discuss the overarching concept of private spheres. Finally, this comment proposes an interim solution borrowing well-established international privacy principles[5] to promote transparency and choice in data use and collection. The ultimate goal of the proposal is to empower workers as full participants in the economic, social and political processes necessary to overhaul the broken legal tools, which fail to protect employee privacy.

I. THE LEGAL PROBLEM — COLLAPSED DISTINCTIONS BETWEEN PRIVATE AND WORK SPHERES RENDER LEGAL DOCTRINES OF PRIVACY LAW FUTILE IN THE EMPLOYMENT RELATIONSHIP

The legal standard to determine an invasion of privacy is insufficient to fully capture the complexities of the modern employment relationship.[6] The current standard exacerbates the existing power imbalance between employer and employee because "it gives the employer the power to determine its liability simply by modifying the work environment to decrease employee privacy expectations."[7] Nevertheless, it is not enough to redraft the current legal tests because the central concepts in privacy doctrine are rooted in a distorted legal fiction of a distinct "private sphere" that is unrealistic to provide protection in the modern workplace where clear distinctions between work and private lives have collapsed.[8]

Under the existing regime, employee privacy rights have significantly diminished[9] and current workplace organization trends are

5. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, THE ORGANIZATION OF ECONOMIC COOPERATION & DEVELOPMENT, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines.

6. Angerer, *supra* note 1, at 3-4 (advocating for increased state action to protect employee privacy "[m]oreover, employment law has, unfortunately, proven to be woefully inadequate in promoting and protecting employee privacy at the workplace.").

7. Larry O. Natt Gantt II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 424 (1995).

8. Ken Strutin, *Social Media and the Vanishing Points of Ethical and Constitutional Boundaries*, 31 PACE L. REV. 228, 229 (2011) (advocating for a paradoxical shift in perceptions to meet the spatial complexities of the "virtual socialscape exists at right angles to the physical world, and so our perceptions must bend accordingly.").

9. Angerer, *supra* note 1, at 5 (elaborating that "scholars have described current employee privacy under the law as: 'near extinction,' usually lacking a remedy for employees, and approaching the point where, 'employers can become Big Brother'").

likely to provide employees with a false sense of security about their privacy rights.[10] The increased capabilities of new monitoring technologies, coupled with the risk of employee misconception of their legal rights, threaten to unnecessarily complicate workplace dynamics and undermine the limited privacy protections available to employees.[11]

Two critical issues remain unsettled in employment privacy law and threaten to give rise to a wave of unnecessary litigation if technological trends and work structures continue current trajectories. First, modern technologies complicate the application of privacy law in the employment relationship because monitoring technologies can collect more data than ever before, thus unnecessarily increasing the risk of invading an employee's "private sphere." Second, both employer and employee expectations of their working relationship are not in harmony with actual legal rights to privacy.

II. ANALYSIS

Meaningful privacy protections for workers are often thwarted by the very legal standards established to create privacy rights.[12] Employers effectively control the scope of an employee's reasonable expectation of privacy by manipulating practices and procedures in the workplace. This uneven balance of power and information in favor of the employer, has potentially harmful repercussions such as "the impact of excessive and undisclosed monitoring in employee morale."[13]

Finally, the reasonable expectation of privacy standard as applied, does not mesh with actual practice and employee perceptions. Businesses are global and mobile, requiring a flexible workforce willing to give up ever-increasing amounts of their personal time to contribute their labor.[14] Twenty-first century workers rarely enjoy the seclusion of a true private sphere and converge their work and private

10. Ciocchetti, *supra* note 4, at 290–91 (arguing that "it is important that the law recognize the power of contemporary monitoring technology, the ever-increasing number of hours contemporary Americans spend at work, and the impact of excessive and undisclosed monitoring on employee morale. Such recognition must lead to a rebalancing of current legal provisions to reflect the realities of the twenty-first-century workplace").

11. *Id.* at 357-58 (explaining that "[i]t is an easy case to make that the current legal regime is inadequate to protect an employee's every move from the scrutiny of today's monitoring practices").

12. Angerer, *supra* note 1, at 4 (reiterating that "[m]oreover, employment law has, unfortunately, proven to be woefully inadequate in promoting and protecting employee privacy at the workplace").

13. Ciocchetti, *supra* note 4, at 290–91.

14. Gantt, *supra* note 7, at 424.

lives into their daily routines. These trends towards comingled work structures and technological advancements in monitoring threaten to erode employee privacy rights because any employee's reasonable expectation of privacy is subject to modification by the employer.

A. Modern Technologies Complicate Effective Application of the Traditional Privacy Tests

Modern monitoring technologies collect more data than ever before and present an unprecedented risk of invading employee privacy. These advances in the capacity of monitoring technologies and their pervasive use to monitor employees present an unprecedented risk of invading employee privacy.[15] These new and emerging technologies are problematic in the employment context because they facilitate privacy invasions into "the personal lives of employees with little or no chance of detection," and "[allow] employers to manipulate, access, and collect information about employees in greater amounts than previously possible."[16]

Many savvy employers leverage the work related technology they provide to their employees as a tool to closely monitor employees.[17] These electronic monitoring efforts may inspect employee communications and movements, including phone calls, e-mails, internet usage and Global Positioning System (GPS) enabled devices. Even when employers have legitimate business reasons to justify monitoring,[18] the risk of collecting incredibly sensitive personal information of workers that are in turn subject to various overlapping privacy regimes and government agencies may curb the savvy employer's appetite for widespread use of these disruptive technologies.

Unfortunately these technological advancements "outpace existing

15. Ciocchetti, *supra* note 4, at 357–58(explaining that "[i]t is an easy case to make that the current legal regime is inadequate to protect an employee's every move from the scrutiny of today's monitoring practices").

16. Gantt, supra note 7, at 346.

17. *See* Melinda L. McLellan et al., *Wherever You Go, There You Are (with Your Mobile Device): Privacy Risks and Legal Complexities Associated with International "Bring Your Own Device" Programs*, 21 RICH. J.L. & TECH. 1, 30 (2015). Consistent with the fractured privacy regulatory regimes in the United States, new technologies and BYOD policies are subject to multiple potentially overlapping federal statutes including: Electronic Communications Privacy Act; the Stored Communications Act; and the Computer Fraud and Abuse Act.

18. Greg Mgrditchian, *Employment & Social Media Privacy: Employer Justifications for Access to "Private" Material*, 41 RUTGERS COMPUTER & TECH. L.J. 108, 133 (2015) (elaborating that legitimate business concerns may include: "concern[] with the public image of their business, the economic viability of the company, the protection and safety of other employees and customers, [and] avoiding lawsuits").

legal sources of privacy protection, as courts seem unwilling or unable to protect employees from purely electronic invasions of privacy."[19]

1. BYOD/Single Device Issues

The common practice of an employee using a single internet capable device to complete both personal and professional tasks[20] exemplifies the ways in which a delineable zone of work is inadequate to address the realities of modern employment trends.

"Bring Your Own Device" (BYOD) policies have evolved as the "go-to standard in most workplaces."[21] Corporate BYOD policies encourage a work culture where employees are available to perform work related tasks at any hour.[22] The practice of comingling personal and work related data on the same device may be mitigated somewhat through geofencing software,[23] but ultimately BYOD highlights just how entangled the private and work realms have become.[24]

BYOD policies demonstrate the interests at odds in employment privacy and technological advancements—the employee interest in personal data privacy is pitted directly against the employer cyber security and trade secret concerns.[25] The technology also presents a complicated conceptual challenge to existing employment privacy laws and practical challenges with attempts to "disentangle the personal from the professional when it comes to protecting and monitoring data on their employees' devices—and this premise assumes it is even possible to make a meaningful distinction between the two."[26]

2. GPS Technology

Another technological advancement with serious employment

19. Gantt, *supra* note 7, at 346.

20. McLellan et al., *supra* note 17, at 1.

21. Freeland Cooper, Foreman LLP, *BYOD? Avoiding the Pitfalls of Employee Use of Personal Devices*, 22 No. 13 CAL. EMP. L. LETTER 10 (Oct. 8, 2012).

22. *See* McLellan et al., *supra* note 17, at 3 (explaining that "BYOD is touted as 'combining workforce mobility and 'always reachable' boosts in employee productivity with possible savings on corporate telecom services and device spending.'").

23. Roman Foeckl, *Why Geofencing Will Become the Next Endpoint Security Innovation*, SC MAGAZINE UK (May 6, 2015), http://www.scmagazineuk.com/why-geofencing-will-become-the-next-endpoint-security-innovation/article/413037/. "Geofencing can restrict access to devices or applications while inside a company's perimeter, making it impossible for devices outside the perimeter to access the network."

24. *See* McLellan et al., *supra* note 17, at 3–4 (reiterating the purported benefits of BYOD "as a boon to employees [who] want to use their own smartphones and tablets at work for convenience as the border between work and personal or recreational activities continues to blur").

25. *Id.* at 4–6.

26. *Id.* at 4.

privacy implications is the rise in devices that include Global Positioning System (GPS) technology. GPS is a satellite-based navigation system in which a "receiver can accurately determine its position within a few meters."[27] GPS devices in company issued cell phones and vehicles "allow . . . employers to keep tabs on employee hours or vehicle travel."[28] The potential privacy invasions at risk with GPS technology are even more problematic than standard surveillance because of "the extraordinary capacity of a GPS device to permit '[c]onstant, relentless tracking of anything.'"[29]

Some state courts have begun to address the privacy implications of GPS tracking technology in the workplace. For example, in *Cunningham v. New York State Dep't of Labor* the court ordered suppression of GPS evidence because the public employer failed to "mak[e] a reasonable effort to avoid tracking an employee outside of business hours."[30] The court created a categorical GPS exception to a general rule that permits employers to use "permissible portion[s] of the search" even when the search as a whole exceeds its permissible scope.[31] The court reasoned that the very nature of GPS technology to monitor intimate details makes the previous rule that favored employers simply "inapplicable to GPS searches."[32]

Additionally, in *Haggins v. Verizon New England, Inc.* union employees were allowed to challenge their employer's use of GPS tracking software as both an unfair labor practice and an invasion of privacy.[33] In *Haggins*, the court did not decide the privacy issue on its merits, but proceeded to outline the difficult test an employee seeking privacy protections must meet.[34] The Massachusetts test required employees to show "not only that the [employer] unreasonably, substantially and seriously interfered with [their] privacy by disclosing facts of highly personal or intimate nature, but also that it had no

27. Adam Koppel, *Warranting A Warrant: Fourth Amendment Concerns Raised by Law Enforcement's Warrantless Use of GPS and Cellular Phone Tracking*, 64 U. MIAMI L. REV. 1061, 1063–64 (2010).

28. *Id.* at 1064.

29. Cunningham v. New York State Dep't of Labor, 21 N.Y.3d 515, 523 (2013) (quoting People v. Weaver, 12 N.Y.3d 433, 441 (2009)).

30. *Id.*

31. *Id.* (noting that the "extraordinary capacity" of the technology makes it categorically unfit for the general rule).

32. *Id.*

33. Haggins v. Verizon New England, Inc., 736 F. Supp. 2d 326, 328-30 (D. Mass. 2010) *aff'd*, 648 F.3d 50 (1st Cir. 2011).

34. Haggins v. Verizon New England, Inc., 648 F.3d 50, 55 (1st Cir. 2011) (holding that the Labor Management Relations Act preempted the employee's privacy claim and that resolution of their claim required interpretation of their collective bargaining agreement).

legitimate reason for doing so."[35] This reiteration of the reasonableness requirement is particularly challenging for non-union employees, because without independent contractual protections the default contours of reasonableness rely on merely on industry standards.[36]

3. The Internet of Things

The number of devices connected to the internet has increased exponentially,[37] and the proliferation of these devices as tools to increase work productivity create heightened privacy risks in the modern employment relationship.

The term Internet of Things ("IoT") broadly encompasses the "network of physical objects embedded with electronics, software, sensors and connectivity" which in turn "enable [those objects] to achieve greater value and service by exchanging data with . . . [an] operator."[38] For example, modern objects like fitness trackers, cell phones, refrigerators, thermostats, Amazon's "dash button,"[39] cars, and even children's toys[40] are part of the growing Internet of Things because they connect to the internet and exchange data to perform specific functions.[41]

In 2015, the Federal Trade Commission ("FTC") estimated the

35. *Id.* (quoting Martinez v. New Eng. Med. Ctr. Hosps., Inc., 307 F. Supp. 2d 257, 267 (D. Mass. 2004).

36. *Id.* at 55–56 (noting that a key factor "to determine the reasonableness of the interference likely will require resort to the custom and usage of the parties and their particular industry practices").

37. *See* Federal Trade Commission Remarks, *How to Regulate the Internet of Things Without Harming Its Future*, 2015 WL 3541727, at 3 (May 21, 2015) (showing the trend that "[r]esearchers have estimated 900 million devices were connected to the Internet in 2009, increasing to 8.7 billion devices in 2012, and now up to 14 billion devices today" and predicting the trend growing "that by 2020 there will be 25 to more than 30 billion devices connected to the Internet of Things").

38. *Id.* at 1 (quoting *Internet of Things*, WIKIPEDIA, http://en.wikipedia.org/wiki/Internet_of_Things).

39. Amazon's "Dash Button" is a plastic button that allows "shoppers to reorder frequently used domestic products like laundry detergent or paper towels with the click of a real-life button." Ian Crouch, *The Horror of Amazon's New Dash Button*, THE NEW YORKER (Apr. 2, 2015), http://www.newyorker.com/culture/culture-desk/the-horror-of-amazons-new-dash-button.

40. Mattel's "Hello Barbie" is a doll connected to the internet featuring speech recognition and progressive learning features which allow a user to engage in "real-time artificially intelligent conversations" with a doll that is constantly transmitting the information it receives from the user to have more personalized "conversations." *Hello Barbie Frequently Asked Questions*, http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/12/hellobarbie-faq-v3.pdf.

41. *See* Andy Greenberg and Kim Zetter, *How the Internet of Things Got Hacked*, WIRED MAGAZINE (Dec. 28, 2015), http://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/.

number of internet connected devices to be 14 billion,[42] put another way "[t]here are currently more devices connected to the internet than people on the planet."[43] As these devices become more prolific throughout the global economy, they have also found their way into the employment relationship through telepresence and wearable technology.[44] If market trends continue, some hypothesize fundamental "change[s] [in] the organization of work and our workspaces" where workers rely on "algorithms embodied as robots or avatars [to] provide solutions to problems [and] facilitate decision-making."[45]

These devices have the ability to track incredibly intimate details about an employee[46] and yet their development, use, and proliferation continue without regulatory protections. In January 2015, the FTC suggested that because the industry is still in its infancy, specific legislation targeting the industry would be unduly burdensome to developers and ineffective to protect consumers.[47]

The unprecedented ability of devices in the Internet of Things to both monitor and interact with private details about employees combined with the lack of federal regulation in the area presents significant risk of invasion of employee privacy.

4. Social Media Usage in Workplace

Finally, the pervasiveness of social media presents additional technological complications to workplace privacy where the "legal implications of this movement are still evolving daily."[48] Social

42. Federal Trade Commission Remarks, *How to Regulate the Internet of Things Without Harming Its Future*, 2015 WL 3541727, at 3 (May 21, 2015).

43. *Id.*

44. Jason Corsello, *What the Internet of Things Will Bring to the Workplace*, WIRED MAGAZINE, http://www.wired.com/insights/2013/11/what-the-internet-of-things-will-bring-to-the-workplace/.

45. *Id.*

46. *See* Federal Trade Commission, *Internet of Things: Privacy & Security In a Connected World* (Jan. 2015),
https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
(explaining that "one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment").

47. *See generally* Federal Trade Commission, *Internet of Things: Privacy & Security In a Connected World* (Jan. 2015),
https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

48. Mgrditchian, *supra* note 18, at 109.

media[49] sites like Facebook, Twitter, YouTube, and LinkedIn "gained prominence rapidly" and have drastically changed the tone and impact of life in the Information Age.[50] As of September 2016, Facebook had over 1.79 billion active users, and of those active users an average of 1.09 billion people used a mobile device to access the site each day.[51]

The massive popularity of online sharing combined with the estimate that "employees spend about [an average of] one to two hours a day using the Internet for personal use" exposes a potentially vast workplace privacy issue as "it is not hard to imagine that in today's society, where technology and communication join at the proverbial hip, social media use during work hours is a widespread issue."[52]

Employer and young professional interests in social media could converge as the ability to use social media during work becomes an exchange for payment.[53] Surprisingly, Millennial workers place such a high value on "social media flexibility" that one poll revealed that 45% of participants would accept a position with lower wages in exchange for a "more liberal policy toward personal tech devices and access to social media at work."[54] Social media has developed into a widespread form of instantaneous communication,[55] and the complicated interwoven personal and professional functions they serve also undermine the legal myth of a purely private sphere.

An employer may inadvertently capture social media data on its employees when an employee accesses the site on a company network, or an employer may intentionally capture this data as part of its routine employee monitoring policy. Employers justify monitoring the social media activity of employees as necessary to address legitimate business

---

49. Cal. Lab. Code § 980 (defining social media as "an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations").

50. Strutin, *supra* note 8. at 287–89 (concluding that the movement towards social media is a "new part of the Information Age, the Social Media Era. It is the time of quantum computing and the specter of nearly a billion personal profiles online").

51. Facebook Newsroom, Statistics (2016), http://newsroom.fb.com/company-info/.

52. Mgrditchian, *supra* note 18, at 116 (describing the pervasiveness of internet use– "[s]tudies show that, on average, employees spend about one to two hours a day using the internet for personal use").

53. Strutin, *supra* note 8, at 288.

54. Mark I. Schickman, *Dude How Fast Is Your Connection?*, 21 NO. 20 CAL. EMP. L. LETTER 3 (Jan. 23, 2012). "CISCO [] polled 2,800 college students and young professionals, [and] it found that social media flexibility was a significant factor in job choice: 40 percent of the college students and 45 percent of the employed 20-somethings said they would take a lower-paying job with a more liberal policy toward personal tech devices and access to social media at work."

55. Mgrditchian, *supra* note 18, at 116 (explaining that "[t]he world's two most popular social media sites, Facebook and Twitter, have approximately 1.11 billion and 232 million active users, respectively.").

concerns such as productivity, safety, and reputation.[56] However, employers who engage in extensive social media monitoring should beware the risks of obtaining too much information.

For example, in 2010 the National Labor Relations Board ("NLRB") began policing employers who terminated employees because of their social media activity.[57] The NLRB investigated and prosecuted employers with written social media policies that had the potential to violate the National Labor Relations Act, because the policies "interfered with the rights of employees . . . to discuss wages and working conditions with co-workers."[58] Due to the influx and uncertainty in the law, employers may now refrain from establishing written social media policies to avoid potential liability from the NLRB.[59]

B. Workers May Lack Understanding of the Implications of Privacy at Work

The daily reality of employee interactions with their employer, coworkers, schedules and environment fosters misconceptions about the true privacy risks employees face during work and the effectiveness of any legal remedy. The business trends to incorporate personal amenities into the workspace and encourage on-call but "flexible" work schedules may signal to employees that they have some autonomous control over their personal privacy while at work.

1. Corporate Campus Operates as a Company Town

First, the environment of a modern corporate campus intentionally bleeds the lines between traditional "private sphere" and "work" activities much like the Industrial Era company town.[60] At first glance this blended work and private environment may appear altruistic, but

56. *Id.* at 133 (noting that an employer's legitimate business concerns include: "concern with the public image of their business, the economic viability of the company, the protection and safety of other employees and customers, avoiding lawsuits, and many other things that can affect an endless amount of people").

57. *The NLRB and Social Media*, NATIONAL LABOR RELATIONS BOARD: NEWS & OUTREACH: FACT SHEETS, https://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media (explaining that "[i]n four cases involving employees' use of Facebook, the Office of General Counsel found that the employees were engaged in "protected concerted activity" because they were discussing terms and conditions of employment with fellow employees.").

58. *Id.*

59. Scott A. Faust, *Electronic Workplace Monitoring and Surveillance*, Practical Law Practice Note, 1-506-8862 (advising employers to "use caution before taking any personnel or legal action against an employee for Facebook or other social media posts in light of recent decisions by the [National Labor Relations Board] NLRB.").

60. *See infra* section IV A 2 ii (discussing work organization of company towns).

its rise as the new social norm threatens to repeat history and block employees from any reasonable expectation of privacy.

One-way employers entice modern workers to devote more time and energy to company productivity is through benefits and accommodations. These benefits encourage employees to rely on their employer for tasks that were once reserved for private life after working hours.

For example, some of the benefits Silicon Valley companies provide include on site gyms, free or subsidized meals, dry cleaning services, scheduling last minute babysitters for sick kids, or even house cleaning services.[61] The inclusion of these traditionally private individual responsibilities into the fabric of work life has created a corporate campus that resembles a modern day company town. Because the corporate campus arguably serves as a blended space for individuals to contribute productive labor and fulfill personal needs, employees may unknowingly sacrifice their privacy protections because they lack reasonable privacy expectations while using employer services on employer property.

2. Flexible Work Schedules May Warp Expectations

Second, the flexible yet continuous schedules of modern work may give employees a false illusion that autonomy to control the hours in which they work also carries implicit rights to privacy. Employees dedicate an ever-increasing number of hours to their work,[62] and simultaneously manage their personal and business responsibilities from the same devices. Because the "new world order is a 24/7 workplace"[63] where employees are expected to use the internet to work anywhere and anytime,[64] some may believe that the brief moment spent answering a late night work email from home and then setting up a confidential doctor's appointment the next minute means that the latter is protected from an employer's prying eyes. This trend to more flexible but overall longer workdays only "[intensifies the] need for

61. John C. Goodman, *Silicon Valley Employers Go Wild With Lavish Employee Benefits*, FORBES (Oct. 30, 2012), http://www.forbes.com/sites/johngoodman/2012/10/30/silicon-valley-employers-go-wild-with-lavish-employee-benefits/.

62. Ciocchetti, *supra* note 4, at 290–91.

63. Michelle Lee Flores, Cozen O'Connor, *7 'Gotchas' of the 24/7 Workplace*, 25 No. 10 CAL. EMP. L. LETTER 4 (Aug. 24, 2015).

64. Claire Cain Miller, *Silicon Valley Is Growing Up, Giving Parents a Break*, THE NEW YORK TIMES (Nov. 25, 2015), http://www.nytimes.com/2015/11/26/upshot/silicon-valley-is-growing-up-giving-parents-a-break.html?_r=0 (explaining that "[l]ong hours in the office and the expectations of being connected at home are familiar to workers across industries, not just Silicon Valley.").

workplace privacy," because employees spend less time than ever before in the traditional sanctity of privacy and thereby relinquish more privacy protections to their employer. [65]

3. False Sense of Security of Interconnected Lives and Autonomy

Ultimately the flexibility of the blended work environment that incorporates traditionally "private" duties into the corporate campus, coupled with the flexible work schedule, may give employees a false sense of security that their lives are interconnected only when they choose for them to be. As any recognizable distinctions between private and work spheres continue to collapse, the new social norm that emerges has the potential to completely unravel the legal standards of privacy in the employment relationship.

As mentioned above, workers may think they are bargaining for the benefit of flexible technology and social media policies when they are actually undermining their own reasonable expectations to privacy.[66] That bargain has unexpected consequences for employee privacy; in reality "employees who use social media to post during work hours, or discuss activities that took place during work hours, enjoy the weakest protections under the law and have a severely diminished expectation of privacy."[67]

The trend towards a blended, amorphous work environment has serious consequences for employers and employees. This structure weakens traditional distinctions of determining the privacy protection of a space based on its purpose and function. As societal roles for spaces become amorphous, these societal shifts transform the threshold legal consideration of privacy claims and further erodes the limited protection available to workers.

III. BACKGROUND

A. Traditional Privacy Law in the Employment Relationship

Privacy protections in the United States are enforced through a fragmented regulatory scheme where certain industries or categories are often subject to overlapping or even conflicting regulations.[68] Privacy in the employment relationship is no different.[69] In the

65. Gantt, *supra* note 7, at 424.
66. *See* Schickman, *supra* note 56.
67. Mgrditchian, *supra* note 18, at 132.
68. Angerer, *supra* note 1, at 9.
69. *Id* at 7–9. (explaining that the "patchwork" of statutory attempts to provide workers with more privacy protections allow for a wide degree of variance with only "nominal" protection).

employment context, rights to privacy may arise from various sources: the United States Constitution, federal statutes, state law, common law, and contract.[70]

Claims of workplace privacy invasions are highly factual inquiries that "must be addressed on a case-by-case basis."[71] The specific factual situation at issue requires courts to evaluate each particular situational context to determine the appropriate source of law to apply.[72]

For instance, privacy invasions made by public employers are held to a Constitutional standard, whereas private employers are not.[73] So while an invasion of privacy claim against a public employer is subject to the Fourth Amendment protection from unreasonable search and seizure by the government,[74] the same claim against a private employer may only be subject to state regulations.[75] There is no universal legal standard of what employer actions will constitute an invasion of employee privacy, and due to the nature of the inquiry there is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."[76]

1. General Framework to Determine Employment Privacy

Despite the various sources of employment privacy law, judicial interpretation of the invasion of employee privacy remains similar. Generally courts will consider three factors to determine whether an employee's right to privacy has been violated: (1) whether the employee had a reasonable expectation of privacy; (2) the extent of the employer's intrusion on that reasonable expectation; and (3) the employer's legitimate business reasons for the intrusion.[77] Most courts

70. *Id.* at 7–9, n.67 (explaining that "[o]ther claims, such as intentional infliction of emotional distress, negligent infliction of emotional distress, and breach of contract, have also been used to attempt to remedy invasions of privacy by employers.").

71. Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 317 (2010) (quoting O'Connor v. Ortega, 480 U.S. 709, 718 (1987).

72. *See* Mgrditchian, *supra* note 18, at 113–14; O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (explaining the role of establishing contours of the workplace, "[b]ecause the reasonableness of an expectation of privacy, as well as the appropriate standard for a search, is understood to differ according to context, it is essential first to delineate the boundaries of the workplace context.").

73. Mgrditchian, *supra* note 18, at 113–14.

74. *Ortega*, 480 U.S. at 725–26. The *Ortega* case is the most influential case of unreasonable search and seizure by the government as an employer. In the opinion Justice O'Connor established the Constitutional requirements of the 'special needs doctrine,' thereby permitting the government as an employer to invade employee privacy under a tiered standard of reasonableness.

75. Katz v. United States, 389 U.S. 347, 350–51 (1967).

76. *Ortega*, 480 U.S. at 715.

77. *Id.* at 725–26.While *O'Connor v. Ortega* addressed an unwarranted search by the

tend to weigh an employer's legitimate business interest more heavily than the employee's privacy interest.[78] This bias in favor of employers reflects the idea that activity in the workplace is subject to public gaze and that the "workplace exists [only] for work purposes."[79]

i. Common Law – Intrusion Upon Seclusion Tort

The tort of intrusion upon seclusion is a vestige of the first common law recognition of privacy[80] and remains the "most commonly [used tort] to protect employee privacy against excessive employer intrusion."[81] Intrusion upon seclusion, or the "right to be let alone," was developed to "[protect] the individual from unwanted social invasions."[82] The jurisprudence that developed the right to be let alone describes privacy interests as "safe zone[s]," "private realm[s]," and a "private sphere."[83]

Intrusion upon seclusion "creates a cause of action when one intrudes 'upon the solitude[84] or seclusion of another or h[er] private affairs or concerns' if the intrusion is 'highly offensive to a reasonable person.'"[85] This protected right to solitude "enables people to rest from the pressures of living in public and performing public roles."[86] Critics of the tort argue that the element requiring the degree of the intrusion to be "highly offensive" improperly places emphasis "not [on] privacy, but outrage."[87]

Courts generally adhere to the subtle, yet overpowering concept of personal space and "recognize intrusion upon seclusion tort actions

government as employer, it serves as the touchstone framework for most employment privacy tests. "In the case of searches conducted by a public employer, we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace." *Id.* at 719–20.

78. *Id.*

79. *Id.*

80. Solove, *supra* note 2, at 483, 552–53 (explaining the historical significance of the intrusion upon seclusion claim as "[o]ne of the torts inspired by Warren and Brandeis's article ['The Right to Privacy']").

81. Angerer, *supra* note 1, at 9.

82. Solove, *supra* note 2, at 553.

83. *Id.* at 553–54. Despite the language supporting privacy interests as a definable space or zone, Daniel Solove contends "intrusion [upon that zone] need not involve spatial incursions."

84. *Id.* at 554. "[S]olitude, [means] the state of being alone or able to retreat from the presence of others."

85. *Id.* at 553.

86. *Id.* at 555.

87. Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221, 228 (1996) (arguing that "[t]he inescapable conclusion is that what the law of intrusion actually regulates is not privacy, but outrage. The law protects freedom from emotional distress, not freedom of informational control").

only when a person is at home or in a secluded place."[88] This approach is essentially "akin to courts recognizing a harm in surveillance only when conducted in private, not in public."[89]

ii. California State Constitutional Approach

The California state constitution established an inalienable right to privacy that employees may use to enforce privacy rights in the workplace.[90] The California reiteration of the three factor balancing test focuses on the parties' interests in light of "established social norms."[91] To determine established social norms, the court inquires into the given "customs, practices, and physical settings surrounding [the potential violation of privacy]."[92]

Even though the "established social norms" requirement has the potential to enhance worker privacy rights, in practice the language operates similarly to the largely ineffective intrusion upon seclusion tort.[93] California courts have even gone so far as to use the social norms consideration to eliminate employee recovery for computer invasions, reasoning that the mere "use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to h[er] use of h[er] employer's computers."[94]

2. The Overarching Concept of a Distinct "Private Sphere" in the Legal Standards

Each of the various legal approaches outlined above are connected by the thematic concept of a protected space, a distinct "private sphere" which is legally discernable and separate from work.[95] The private sphere is understood as a "zone or aura around us to separate ourselves

88. Solove, *supra* note 2, at 555.

89. *Id.* at 555–56.

90. Cal. Const. art. I, § 1. (establishing that "[a]ll 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"); *see also* TBG Ins. Servs. Corp. v. Superior Court, 96 Cal. App. 4th 443, 450 (2002).

91. Cal. Const. art. I § 1.

92. *Id.*

93. TBG Ins. Servs. Corp., 96 Cal. App. 4th at 450. "The 'community norms' aspect of the 'reasonable expectation' element of an invasion of privacy claim is this: " 'The protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens.'"

94. *Id.* at 452–54.

95. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987). The Court presumed that it is possible to "delineate the boundaries of the workplace context" and suggested that the boundaries be a threshold determination.

from others."[96] This theoretical "private sphere" is pervasive in privacy law,[97] and limits the scope of privacy protections in the employment context where clear zones of "private" or "work" are often difficult to delineate.

For example, the intrusion upon seclusion tort was created to "protect a safe zone, a private realm free from intrusions."[98] The tort establishes certain societal values as legal standards to "uphold[] rules of civility and social respect" by respecting other's "territories of the self."[99] To prevail on an intrusion upon seclusion claim, the employer must have "penetrated[100] some zone of physical or sensory privacy [] in violation of the law or social norms."[101] The thematic concept consistent in each legal standard to determine privacy is the reliance on the legal fiction of clear spatial distinctions.

i. The Historical Development of a Legally Protected "Private Sphere"

The concept of a legally protectable "private sphere" is deeply rooted in the original physical manifestation of privacy protections—the family home.[102] The American home represents a clear, legally protected place[103] where a person can expect that their affairs, activities, words and thoughts are free from government intrusion.[104]

The American home became the epicenter for a legally protected private zone in large part because of its perceived importance to establish familial bonds—"the home derives its pre-eminence as the seat of family life."[105] Marital relations and family life are considered

96. Solove, *supra* note 2, at 556.

97. *Id.* at 557–58 (noting that the Supreme Court first articulated the "[v]arious guarantees [by the Bill of Rights] create zones of privacy" in *Griswold v. Connecticut*).

98. *See id.* at 553.

99. *Id.* at 556. "As Robert Post observes, the tort of intrusion upon seclusion upholds rules of civility and social respect. We each have certain 'territories of the self,' and norms of civility require that we respect others' territories."

100. It is troubling that the legal standard to evaluate the degree and setting of the intrusion are couched in terms of male sexual dominance like "penetrate."

101. Ciocchetti, *supra* note 4, at 299.

102. *See* Solove, suprai note 2, at 552 (emphasizing the elevated legal significance of the home "[f]or hundreds of years, the law has strongly guarded the privacy of the home").

103. *See* Griswold v. Connecticut, 381 U.S. 479, 495 (1965) (Goldberg, J., concurring) (finding that "the right 'to marry, establish a home and bring up children' was an essential part of the liberty guaranteed by the Fourteenth Amendment").

104. *See id.* at 484 (reiterating that "[t]he Fourth and Fifth Amendments [act] as protection against all governmental invasions 'of the sanctity of a man's home and the privacies of life'").

105. *Id.* at 495 (noting that "[t]he home derives its pre-eminence as the seat of family life").

the most private and intimate of associations.[106] Courts recognized the "private realm of family life" as a natural zone to protect because of the belief that valuable social bonds are forged in the home.[107] The home became a place of social retreat and solitude "enabl[ing] people to rest from the pressures of living in public and performing public roles."[108]

Three pivotal Supreme Court cases[109] illustrate the development of privacy law in terms of distinct spheres and explore the judicial reliance on the presumed sanctity of the home to anchor new privacy protections.[110]

First, in *Griswold v. Connecticut* the Supreme Court struck down a Connecticut law banning the use of contraceptives on the grounds that the law intruded upon a Constitutionally protected "zone of privacy."[111] The concurrence in *Griswold* found a right to sexual privacy by relying on an earlier Fourteenth Amendment case and re-established that the "right 'to marry, establish a home and bring up children' was an essential part of the liberty guaranteed by the Fourteenth Amendment."[112] The Court expounded on the weight of the marital home as a "particularly important and sensitive area of privacy" and found the mere idea of the government searching the "sacred precincts of marital bedrooms" as "repulsive to the notions of privacy surrounding the marriage relationship."[113]

Second, in *Katz v. United States* the Court held that "wiretapping and eavesdropping by law enforcement agents was a constitutional search that would need to satisfy [] Fourth Amendment prerequisites."[114] *Katz* extended Fourth Amendment protections to telephone conversations, finding that the protection "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[115]

Most noteworthy, Justice Harlan's concurrence in *Katz* articulated

---

106. *Id.*

107. Solove, *supra* note 2, at 555 (elaborating that "a space apart from others has enabled people to develop artistic, political, and religious ideas that have had lasting influence and value when later introduced into the public sphere").

108. *Id.*

109. See Griswold, 381 U.S. at 484; Katz v. United States, 389 U.S. 347, 353 (1967); and Kyllo v. United States, 533 U.S. 27, 28 (2001).

110. *See Katz*, 389 U.S. at 361(Harlan, J., concurring). "[A] man's home is, for most purposes, a place where he expects privacy."

111. *Griswold*, 381 U.S. at 485.

112. *Id.* at 495 (citing Meyer v. Nebraska, 262 U.S. 390, 398 (1923)).

113. *Griswold*, 381 U.S. at 485–86.

114. Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 24 (2004) (summarizing *Katz*).

115. *Katz*, 389 U.S. at 353.

a two-part requirement[116] to determine the reasonableness of a privacy expectation: "[1] that a person have exhibited an actual (subjective) expectation of privacy and, [2] that the expectation be one that society is prepared to recognize as 'reasonable.'"[117] *Katz* "represents a great touchstone in the law of privacy" because Justice Harlan's test "extend[ed] beyond the confines of the Constitution [and] found its way into common law and statutes" expounding privacy protections.[118] The additional requirement that a privacy invasion must be subjectively and objectively reasonable has significantly shaped the development and focus of privacy rights.[119]

Katz also represents a failed attempt to expand the right of privacy beyond the notion of the static home.[120] The Court famously declared that the right to privacy should be attached to a person—"[f]or the Fourth Amendment protects people, not places."[121] Yet, ultimately the Court declined to expand privacy into a "general constitutional 'right to privacy,'" preferring to leave these protections "largely to the law of the individual States."[122]

Third, in *Kyllo v. United States*, the Court held that thermovision imaging of a private home constituted an unlawful search under the Fourth Amendment.[123] Again the Court reiterated the importance of the home as an anchor to privacy rights—"in the sanctity of the home, all details are intimate details."[124] The Court also reiterated its subjective-objective standard from *Katz* that a privacy intrusion occurs "when the [intruder] violates a subjective expectation of privacy that society recognizes as reasonable."[125]

Ultimately, these three Supreme Court cases illustrate how the development of privacy rights in the United States are intrinsically linked and entangled with the concept of a "private sphere."[126]

---

116. *Kyllo*, 533 U.S. at 34. Justice Scalia directly addressed critics in his opinion noting that the two-part requirement "has often been criticized as circular, and hence subjective and unpredictable."

117. *Katz*, 389 U.S. at 361.

118. *Peter Winn, Katz and the Origins of the "Reasonable Expectation of Privacy" Test, 40 MCGEORGE L. REV. 1 (2009).*.

119. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (establishing reasonableness of a privacy interest as precedent by adopting Justice Harlan's two prong test in the majority opinion).

120. *Katz*, 389 U.S. at 351 (noting that "effort[s] to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case").

121. *Id.*

122. *Id* at 350–51.

123. Kyllo v. United States, 533 U.S. 27, 40 (2001).

124. *Id.* at 28.

125. *Kyllo*, 533 U.S. at 33.

126. *Id.*; *Griswold*, 381 U.S. 479.

ii. The "Private Sphere" Collides with Workplace Realities

The theoretical concept of a discernable private zone remains central to the legal analysis of a workplace privacy invasion claim. The Supreme Court explains that the "essential" first step of such an inquiry is to "delineate the boundaries of the workplace context."[127] This first step perpetuates a fallacy that the American employment relationship can be carved into a clearly designated and separate "work space."[128] The Court describes workplace boundaries as "those areas and items that are related to work and are generally within the employer's control."[129] The legal standard operates in terms of discernable spatial boundaries, even when modern and historical examples of work organization show the weakness of the standard's conceptual underpinnings.

For example, Industrial Era work structures such as company towns and "Fordism"[130] practices highlight how even more traditional workplace boundaries bled into the private sphere. Employers that operated company towns exerted influence in both the professional and personal zones of its employees. For instance, in the coal mining and steel industry "employers [would] pay workers in scrip redeemable only at the company store, located in the company town where employees lived and worked."[131] The legal approach to discern workplace boundaries as a prerequisite to privacy is inadequate to protect employees in these types of complicated employment relationships. The work structure of a company town undercuts even the quintessential private sphere, the home, because all areas of the company town are in some sense related to the work and remained within the employer's control.

The Ford Motor Company ("Ford") serves as another early example of an employment relationship that intentionally blended the "private" and "work" spheres.[132] Ford implemented a policy to pay its

127. O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

128. *Id.* at 715–16 (explaining workplace boundaries in a physical example "[a]t a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace").

129. *Id.* at 715.

130. Defined by the Merriam Webster Dictionary as "a technological system that seeks to increase production efficiency primarily through carefully engineered breakdown and interlocking of production operations and that depends for its success on mass production by assembly-line methods." '*Fordism' Definition*, http://www.merriam-webster.com/dictionary/Fordism. The actual employment practices and policies of Henry Ford have also been referred to as "corporate paternalism." *See* Leo E. Strine, Jr., *A Job Is Not A Hobby: The Judicial Revival of Corporate Paternalism and Its Problematic Implications*, 41 J. CORP. L. 71, 78 (2015).

131. Strine, *supra* note 141, at 78.

132. Angerer, *supra* note 1, at 36.; Strine, *supra* note 141, at 78 (elaborating that

employees twice the average wage on the condition that they "conformed to Henry Ford's religious and moral ideals."[133] The structure of the employment agreement meant that even in the sanctity of their own home, a Ford employee could not fully enjoy a true zone of familial privacy because company investigators would "visit worker's houses, conduct interviews, and perform inspections" to guarantee that employees "liv[ed] their lives according to middle class, Protestant values."[134] These types of invasive practices blur workplace boundaries and in turn diminish privacy rights because employers can "not only control[] employee behavior during the work days [] but also attempt[] to control what their workers did with their scarce free time."[135]

Even though the example of the Ford Motor Company's corporate paternalism[136] seems extreme, it highlights the potential flaws in hinging worker privacy rights on a fictional "private sphere" that is separate and distinct from work. As the modern employer practice of extensive employee monitoring through technology[137] is "becoming ubiquitous,"[138] the legal fiction of a private zone of retreat is again at odds with protecting employee privacy.

Today, on the whole, it is difficult for employees to gain meaningful privacy protections under the general legal standards.[139] These standards reflect judicial adherence to a legal fiction that cannot adequately account for the blurred lines between "zones." As a practical matter, in employment privacy "for the most part, private employers must intrude into very private places — such as restrooms or locker rooms — to face liability for [a privacy claim]."[140]

Typical workplace privacy issues arise from employer actions, such as physical and psychological testing, investigatory interrogations and searches of persons/spaces, monitoring and surveillance, inquiries

---

"Corporate paternalism was not an incidental aspect of the scheme: paying workers in scrip, and controlling where they could live, enabled employers to police all aspects of their workers' lives").

133. *Id.* at 81.

134. *Id.*

135. *Id.* at 73.

136. *Id.* (arguing that transition to industrial capitalism in American bred "a new strain of feudalism returned in the form of something that might charitably be called 'corporate paternalism'").

137. *Id.* at 75. "Employers are limiting the privacy of workers through technology—such as workplace phone and computer monitoring, cameras, or drug and nicotine testing—for bottom line, business reasons."

138. Ciocchetti, *supra* note 4, at 357.

139. Angerer, *supra* note 1, at 4. "Moreover, employment law has, unfortunately, proven to be woefully inadequate in promoting and protecting employee privacy at the workplace."

140. Ciocchetti, *supra* note 4, at 301.

into prohibitions of off-site conduct and revelations into private matters.[141] Employers offer various legitimate business concerns to justify perceived privacy invasions, including maintaining the public image of the business, ensuring productivity, effectively evaluating work performance, and thwarting potential employee misconduct.[142]

B. Why Employee Privacy Protections Fail at the Threshold Issue: Did the Employee Have a Reasonable Expectation or Privacy?

The threshold issue an employee must establish to proceed with an invasion of privacy claim is whether or not she had an objectively reasonable expectation of privacy. This initial element "offer[s] little help to employees because of the decreased expectation of privacy inherent in any workplace."[143]

Whether or not an employee's expectation of privacy in her work setting is reasonable is addressed on a "case-by-case basis"[144] and considers the "customs, practices, and physical settings [] as well as the opportunity to be notified in advance and consent to the intrusion."[145]

Employers can easily defeat the threshold element of reasonable expectation to privacy through proper planning with prior notice, written consent and practices and procedures.[146] Therefore, the legal standard a plaintiff must meet in a privacy claim is particularly "difficult []to meet in the workplace context,"[147] in part because regular employee monitoring is a widely accepted practice and also because jurisprudence tends to favor employer's interests more heavily in a balancing test for privacy.[148]

1. Notice as a Restriction on "Reasonable Expectation of Privacy"

Notice serves as a protective mechanism to decimate or restrict employee privacy claims because it effectively limits the "reasonableness" of the employee's expectation of privacy before an issue even arises.[149] The following cases involve nearly identical facts but illustrate the problematic jurisprudence that develops when privacy

141. *Id.*
142. Mgrditchian, *supra* note 18, at 133; S. Elizabeth Wilborn, *Revisiting the Public/private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 836–38 (1998).
143. *See* Ciocchetti, *supra* note 4, at 357–58.
144. Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 317 (2010).
145. Ciocchetti, *supra* note 4, at 297–98.
146. *Id.*
147. *Id.* at 299.
148. *See id.* at 290, 357–58.
149. *Id.*

protections are determined state by state.

Two cases involving attorney-client email communications sent using employer issued computers demonstrate the power of notice as a proactive tactic to limit the likelihood of an employee prevailing on a privacy claim.[150] These examples show how even the "oldest of the privileges for confidential communications known to the common law" rooted in a fundamental public policy to promote justice[151] can fall under the reasonable expectation of privacy requirement.

First, in *Holmes v. Petrovich* the court held that an employee did not have a reasonable expectation to privacy in her email communications with her lawyer because she sent the email from a company issued computer and the employer had a computer usage policy that warned the employee that electronic communications were subject to company monitoring.[152] Even though the employee "believed her personal e-mail would be private because she utilized a private password [] and she deleted the e-mails after they were sent," the *Holmes* court analogized the use of a company issued device to communicate with an attorney as "akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [employer] would be privileged."[153] In Holmes, the prior notice from the computer usage policy effectively destroyed the employee's ability to meet the threshold consideration of a reasonable expectation of privacy.[154]

On the other hand, in *Stengart v. Loving Care Agency, Inc*., the court held that the employee did have an expectation of privacy in her email communications with her lawyer.[155] Here the employee also used a work-issued computer to send the communication, but she prevailed because she took "steps to protect the privacy of those e-mails and shield them from her employer" and the computer usage

150. Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1068 (2011)

151. *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (explaining that "the purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice").

152. *See* Holmes v. Petrovich Dev. Co., 191 Cal. App. 4th 1047, 1068 (2011) (explaining the legal test as: "when (1) the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions").

153. *Holmes*, 191 Cal. App. 4th at 1068–69. .

154. *Id.* at 1071 (noting that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated").

155. *See generally* Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 321–22 (2010).

agreement was vague.[156] Despite the employee favorable ruling, the *Stengart* court was careful to limit their holding to prevent an expansion of privacy rights to employees, noting that their legal conclusion "does not mean that employers cannot monitor or regulate the use of workplace computers."[157] While the legal outcome for the plaintiff in *Stengart* was favorable, the court still made sure to note the power of effective prior notice to shape a reasonable expectation of privacy at work.

2. The Power of Consent as a Restriction

Even if an employee can show that their privacy interest is objectively reasonable, their attempt to gain a legal remedy can still fail with proof that they agreed to the possibility of the invasion.[158]

For example, in *Feminist Women's Health Ctr. v. Superior Court* the court reiterated the power of consent to trump invasions—"[c]onsent remains a viable defense even in cases of serious privacy invasions."[159] Here, the employer required a health care worker to demonstrate a cervical self-exam by inserting a speculum into her vagina in front of coworkers and female clients.[160] Even though the court determined that the cervical self-exam "infringe[d] a legally protected privacy interest," the plaintiff signed a consent form to the policy in her new hire documents so her otherwise strong claim to privacy invasion was defeated as a matter of law.[161]

In conclusion, even when a plaintiff employee can successfully meet the threshold requirement that their expectation of privacy be "reasonable", these claims often fail because employers notified the employee of the invasion prior to the incident or obtained signed consent to the invasion.[162]

IV. PROPOSAL

I propose a two-part approach to address the failures of privacy rights in the employment relationship. First I suggest private ordering as an interim solution to address the significant power and informational imbalances between employees and employers. This interim solution aims to educate workers, curb employer monitoring

156. *Id.*
157. *Id.* at 324–25.
158. Feminist Women's Health Ctr. v. Superior Court, 52 Cal. App. 4th 1234, 1249 (1997).
159. *Id.*
160. *See id* at 1237.
161. *Id.* at 1247–49.
162. *See* Ciocchetti, *supra* note 4, at 297–98.

practices, and ultimately allow employees to become meaningful participants in the labor market and political process to advocate for their own privacy rights. Secondly, to truly address the inherent pitfalls of the legal standards of privacy protections in the employment context I recommend a return to the *Katz* approach of conceptualizing privacy as a fluid concept attached to a person, and overhauling the "reasonable" requirement to properly calibrate privacy rights to freedom of informational control as opposed to acceptable social outrage.

First, this private ordering solution borrows from successful privacy standards developed by the international community[163] to create a flexible structure that can lead to a conceptual overhaul of privacy law and elevate the bargaining power of employees.[164] I recommend employers that choose to engage in employee monitoring incorporate the two key consumer choice principles of Collection Limitation and Purpose Specification into their corporate practices.[165]

The Collection Limitation Principle would allow an employee to restrict the data collected about herself by her employer in an "opt-in" choice.[166] Whereas the Purpose Specification Principle would restrict the employer from using the data on an employee in any way not previously disclosed.[167] Incorporating these principles will ensure that organizations limit the collection of potentially sensitive private data about their employees and only use collected data for a disclosed purpose.

Additionally, using these consumer choice principles in the employment context would also help to rectify the power and informational imbalance between an employee and their employer. Although employers have used notice and consent principles mainly as a weapon against employee claims to privacy, these consumer choice

163. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, THE ORGANIZATION OF ECONOMIC COOPERATION & DEVELOPMENT, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines.

164. *See* William J. Kambas, *A Safety Net in the E-Marketplace: The Safe Harbor Principles Offer Comprehensive Privacy Protection Without Stopping Data Flow*, 9 ILSA J. INT'L & COMP. L. 149, 157-58 (2002) (explaining that the OECFP guidelines "represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it").

165. *Id.* at 153, 158 (explaining that the "OECD Guidelines provide guidance to legislative efforts and the development of private sector privacy policies" and explaining each of the eight principles in depth).

166. *See id.* at 158 (explaining that the Collection Limitation Principle "allows data subjects to choose whether or not they want data collected and collection is restricted to consumer preferences").

167. *Id.* at 159 (explaining further that "the Purpose Specification Principle further limits permitted uses to those purposes explicitly stated by the data collector").

driven principles should force nefarious monitoring practices into the public debate for scrutiny as employees become more involved in the decisions about what data is collected and how it is used. This interim step aims to bring both employer and employee expectations of privacy issues and actual practices into alignment.

Finally, the ultimate goal of the quasi-self-regulatory scheme is to improve employer understanding of the potential legal liability inherent in excessive data gathering and educate employees about the reality of their limited privacy protections at work. The private ordering gap filler proposal accounts for the time necessary for technologies to mature before implementing the wide sweeping legislative change necessary to dethrone the "private sphere" distinction and rebuild legal privacy protections for workers. The new regime of privacy protections in the employment context should abandon the objectively reasonable requirement that wrongfully elevates generally acceptable outrage over true privacy and freedom of informational control.

CONCLUSION

In conclusion, modern employment trends exacerbate the inadequacies of the legal standards that could provide privacy protections to workers. Technological advancements increase the amount of sensitive data employers capture from their employees and foster 24/7 work schedules where the legal fiction of a private sphere collapses with the blended realities of twenty-first century work.

Under the current regime of privacy doctrine in the employment context, employers are able to defeat most claims of privacy invasions through careful planning and adherence to industry standards. To remedy the substantial power and informational imbalances between employees and employers an interim quasi-self-regulatory system has the flexibility to address immediate concerns and adapt appropriately to rapidly changing technology. Most importantly, the interim system forces employees into active roles in the negotiation for privacy in the workplace thereby empowering a new group of potential advocates. Advocating with experience in the complex modern employment relationship may support legislative efforts that can do away with static notions of physical zones and return to privacy rooted in the person, and focused on the freedom, of informational privacy.