Northwestern Journal of Law & Social Policy

Volume 16
Issue 1 *Fall*

Article 2

Fall 12-1-2020

Trading Privacy for Promotion? Fourth Amendment Implications of Employers Using Wearable Sensors to Assess Worker Performance

George M. Dery III
California State University Fullerton, gdery@fullerton.edu

Northwestern Journal of Law and Social Policy
Volume 16 (Fall 2020)

Trading Privacy for Promotion? Fourth Amendment Implications of Employers Using Wearable Sensors to Assess Worker Performance

George M. Dery III*

ABSTRACT

This Article considers the Fourth Amendment implications of a study on a passive monitoring system where employees shared data from wearables, phone applications, and position beacons that provided private information such as weekend phone use, sleep patterns in the bedroom, and emotional states. The study's authors hope to use the data collected to create a new system for objectively assessing employee performance that will replace the current system which is plagued by the inherent bias of self-reporting and peer-review and which is labor intensive and inefficient. The researchers were able to successfully link the data collected with the quality of worker performance. This technological advance raises the prospect of law enforcement gaining access to sensitive information from employers for use in criminal investigations. This Article analyzes the Fourth Amendment issues raised by police access to this new technology. Although the Supreme Court currently finds government collection of a comprehensive chronicle of a person's life to constitute a Fourth Amendment search, widespread employee acceptance of mobile sensing could undermine any claim in having a reasonable expectation of privacy in such information. Additionally, employee tolerance of passive monitoring could make employer data available to the government through third party consent. When previously assessing employees' privacy, the Court demonstrated a willingness to accept the needs of the employer and society as justification for limiting workers' Fourth Amendment rights. Ultimately, then, Court precedent suggests that passive monitoring could erode Fourth Amendment rights in the long term.

I. INTRODUCTION

II. MOBILE SENSING STUDY OF WORKER PERFORMANCE

III. FOURTH AMENDMENT CONCERNS CREATED BY EMPLOYERS' PASSIVE MONITORING OF WORKERS' PHONE USAGE, MOVEMENTS, AND PHYSIOLOGICAL DATA

A. Over the Long Term, Widespread Employee Acceptance of Passive Monitoring Could Lessen Privacy Expectations in Shared Information, Undermining Claims that Police Commit a Fourth Amendment Search by Accessing Employer Data

B. Since the Court Has Previously Accepted the Needs of the Employer and Society as Reasons to Significantly Limit Employees' Reasonable Privacy Expectations, the Court Could Allow Passive Monitoring of Employees

C. Employees' Tolerance of, or Submission to, Passive Monitoring, Could Make Employer Data Available to the Government Through Third Party Consent, Making any Fourth Amendment Search Reasonable

IV. CONCLUSION

I. INTRODUCTION

Perhaps, as an employee, you were passed over for a promotion only to see someone less qualified win the position. Maybe you were an employer who sought solid evidence of job performance in order to select employees who would fulfill your organization's mission. Both workers and supervisors may reasonably dread the cumbersome and labor-intensive review process of self-reports and supervisor evaluations that can be both ineffective and biased. Both would benefit from an unbiased assessment system that could increase efficiency and fairness.

Andrew Campbell, a computer science professor at Dartmouth College,[1] decided to test whether monitoring employees' "physical, emotional, and behavioral well-being" with smartphones, fitness trackers and position beacons[2] could help employees seeking promotion.[3] Campbell's idea prompted a study that created a "mobile sensing system" that measured "employee performance with about 80 percent accuracy."[4] Claiming to have objective data provided by the study's wearable devices, an employee could now say, "Here's the evidence that I deserve to be promoted or that my boss is standing in my way."[5]

---

*Professor, California State University Fullerton, Division of Politics, Administration, and Justice; Former Deputy District Attorney, Los Angeles, California; J.D., 1987, Loyola Law School, Los Angeles; B.A. 1983, University of California Los Angeles.

[1] Peter Holley, *Wearable technology started by tracking steps. Soon, it may allow your boss to track your performance*, THE WASHINGTON POST: (June 28, 2019) https://www.washingtonpost.com/technology/2019/06/28/wearable-technology-started-by-tracking-steps-soon-it-may-allow-your-boss-track-your-performance/

[2] *Phones and wearables combine to assess worker performance: Mobile sensing and consumer tech upgrade the employee review*, SCIENCE DAILY, SCIENCE NEWS (June 24, 2019) https://www.sciencedaily.com/releases/2019/06/190624111606.htm (hereinafter "*Science Daily*, Phones and wearables").

[3] *See* Holley, *supra* note 1.

[4] *Id*. This study resulted in the publication of the following paper: Shayan Mirjafari, Kizito Masaba, Ted Grover, Weichen Wang, Pino AUdia, Andrew Campbell, Nitseh Chawla, Vedant Das Swain, Munmun De Dhoudhury, Anind Dey, Sidney D'Mello, Ge Gao, Julie Gregg, Krithika Jagannath, Kaifeng Jiang, Suwen Lin, Qiang Liu, Gloria Mark, Gonzalo Martinez, Stephen Mattingly, Edward Moskal, Raghu Mulukutla, Subigya Nepal, Kari Nies, Manikanta Reddy, Pablo Robles-Granda, Kousuv Saha, Anusha Sirigiri, & Aaron Striegel, *Differentiating Higher and Lower Job Performers in the Workplace Using Mobile Sensing*, 3 PROC. ACM INTERACTIVE MOB. WEARABLE UBIQUITOUS TECH., No. 2, Art. 37, (June 2019).

[5] *See* Holley, *supra* note 1.

While wearable sensors offer the promise of accuracy and fairness, these devices create Fourth Amendment concerns.[6] Indeed, the government has shown an interest in the mobile sensing study. In the study's acknowledgements, the authors noted that the Office of the Director of National Intelligence and an Intelligence Advanced Research Projects Activity contract in part supported its research.[7] Even without such direct government involvement, the study's results could affect Fourth Amendment rights. Widespread acceptance of the collection of personal data involving employees' physical movements, emotions, and habits could erode Fourth Amendment privacy expectations. The sensors used in the study, which ran continuously,[8] collected information such as heart rate, sleep quality, and stress, and therefore accessed personal details encompassing bedroom habits and psychological states.[9] Should providing such information to an employee's supervisor become the norm, Fourth Amendment privacy expectations would be severely diminished.[10] Police, pursuing evidence on issues including alibi, proximity to crime scene, and mental state, could mine a wealth of information by accessing the passive monitoring data employers collected.

To be legally effective, however, such employee consent must be provided voluntarily.[11] In *Differentiating Higher and Lower Job Performers in the Workplace Using Mobile Sensing*, participants' privacy concerns were allayed by giving workers the option to participate in the study.[12] Should commercial and government employers adopt such employee-monitoring technology, supervisors could likewise limit its use to volunteers. This approach, however, brings up its own Fourth Amendment concerns. The researchers' method of obtaining consent—offering workers $750 for participating—hints at a simple way to overcome protests or even hesitation in making this technology common practice in the workplace.[13] Individuals might unwittingly weaken their Fourth Amendment rights by consenting to employer monitoring. Employees might consent to wearing such technology due to their need to obtain cash incentives, because of a hope of remaining competitive for promotions, or simply to keep their jobs. These practical considerations might mask an employee's underlying wish to avoid monitoring.

In Part II, this Article examines the methods and conclusions of the study, *Differentiating Higher and Lower Job Performers in the Workplace Using Mobile Sensing*. Part III discusses Fourth Amendment issues created by this study. Specifically, this Article analyzes whether use of passive monitoring technology in assessing workers' performance may undermine employees' Fourth Amendment rights by eroding reasonable privacy expectations. Part III of this Article also analyzes precedent in which the Court has deemed

---

[6] The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. This Article will focus on Fourth Amendment issues and therefore federal and state laws on employee privacy, as well as individual company policies regarding employee privacy, are beyond the scope of the Article.

[7] *See* Mirjafari, *supra* note 4, at 21.

[8] *Id*. at 8.

[9] *Id*.

[10] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Court's Fourth Amendment privacy analysis is fully explored in Part III, below.

[11] Schneckloth v. Bustamonte, 412 U.S. 218, 248 (1973).

[12] *See* Mirjafari, *supra* note 4, at 6.

[13] *Id*.

employees' privacy to be significantly diminished, often due to the employees' own choices. Finally, this Article explores whether an employee's sharing of personal data may trigger the Court's holdings that persons who share information with a third party assume a risk that the third party might expose the information shared to police. Woven through all of these issues is a concern about the voluntariness of employee decision-making in the context of the competitive workplace. Ultimately, this Article suggests that, while promoting fairness and efficiency, and eliminating bias, are noble goals, the use of wearable technology in reaching such ends could create unintended and adverse Fourth Amendment consequences.[14]

II. MOBILE SENSING STUDY OF WORKER PERFORMANCE

The *Differentiating Higher and Lower Job Performers* study was meant to provide both employers and employees access to hidden factors affecting job performance.[15] Providing employees with precise links between their stress, lifestyle habits, and productivity[16] could "be the key to unlocking the best from every employee."[17] Study coauthor, Andrew Campbell, decided to study mobile sensing of employees after noting that Google, "one of the world's premiere technology companies," still relied on a "traditional performance review" to assess its employees.[18] This standard assessment "typically relies on subjective input such as peer ratings, supervisor ratings and self-reported assessments, which is manual, burdensome, potentially biased and unreliable."[19]

The study's authors sought to examine a "radically new approach" to employee assessment by using phones, wearables, and positional beacons to unobtrusively and objectively measure performance.[20] The researchers developed a "PhoneAgent" application for Apple and Android phones to "continuously and passively" track an employee's "physical activity, location, phone usage (e.g. lock/unlock) and ambient light levels."[21] The researchers also used a Garmin Viviosmart 3 wristband to collect data on "heartrate, heartrate variability, and stress."[22] The Garmin wearable enables employees to enter their weight and automatically measures "step count, calories burned, number of floors climbed and physical activity (e.g., walking, running, etc.)."[23] The study also relied

[14] This Article considers the *Differentiating Higher and Lower Job Performers* study only to explore the Fourth Amendment consequences of passively monitoring employees. The study's scientific claims about performance are beyond the scope of this Article.
[15] *See* Holley, *supra* note 1.
[16] *Id.*
[17] *See Science Daily*, *supra* note 2.
[18] *See* Holley, *supra* note 1.
[19] *See* Mirjafari, *supra* note 4, at 2.
[20] *Id.*
[21] *Id.* at 8.
[22] *Id.* ("Stress" is measured by Garmin's "proprietary black box.").
[23] *Id.*

on Gimbal beacons[24] to measure "time spent at the office and home as well as breaks taken away from a participant's desk."[25]

Over 500 working professionals in the United States used these devices as part of the *Differentiating Higher and Lower Job Performers* study.[26] The professionals, who worked at technology companies and universities, could either participate in the yearlong study for $750 or opt out of the study altogether.[27] Both supervisors and non-supervisors participated.[28] Researchers strictly monitored participants' compliance, calculating the "compliance rate for each participant" by noting whether they had received data from a subject "for each 30 minute time interval."[29] In measuring compliance for 48 30-minute time slots in a 24-hour day, the study's authors found it helpful to "stay in touch with participants" to alert them to any observed problems with compliance rates."[30] At the end of the study, the researchers paid the participants based on their average compliance rate.[31]

Ultimately, the aim of data collection was to "shed light on behavioral patterns that characterize higher and lower performers."[32] The measurements, which were "processed by cloud-based machine-learning algorithms,"[33] produced results both "interesting" and "potentially important."[34] Higher performers generally used their phones less throughout the day.[35] Some higher performers used the phones "less during weekday working hours than during the same period at the weekend,"[36] as well as less during the evenings of workdays.[37] Higher performers also showed differences in their mobility and activity;[38] they were "more active and mobile in comparison to lower performers."[39] Sleep differed between higher and lower performing employees.[40] Higher performers experienced "longer deep sleep periods during survey days and shorter light sleep periods during weekends."[41]

---

[24] *Id*. (Describing beacons as "low energy radio modules that transmit and receive radio signals to and from other Bluetooth enable devices. The PhoneAgent app on the phone implements a Gimbal API library that enables the phone to detect encounters with beacons. To understand the protocol, consider smartphone A and beacon B. When A approaches B, A will receive the signal transmitted by B and report its signal strength. Generally, this signal strength increases as A and B are closer to each other. In this way, we can capture the mobility of participants at work.").

[25] *Id*.

[26] *Id*. at 6.

[27] *Id*.

[28] *Id*.

[29] *Id*. at 9.

[30] *Id*.

[31] *Id*.

[32] *Id*. at 5. The researchers defined workplace performance with reference to a variety of skills, specifically, "*how well workers and employees perform their tasks, the initiative they take and the resourcefulness they show in solving problems*." *Id*. at 3 (emphasis in original). A high performer was one who is "well aware of his or her role in the organization, and executes the underlying tasks and role well." *Id.*

[33] *See* Holley, *supra* note 1.

[34] The researchers asserted their findings offered "important insights into higher and lower performers" and found what they called "a number of interesting results." *See* Mirjafari, *supra* note 4, at 18.

[35] *Id*.

[36] *Id*.

[37] *Id*.

[38] "Mobility" is defined as "movement and places visited." *Id*. at 19. "Activity" is "stationary or moving around." *Id*. at 19.

[39] *Id*.

[40] *Id*. at 20.

[41] *Id*. at 20.

The authors surmised that since "deep sleep is important in memory reactivation and consolidation," accumulating deep sleep might "be a crucial factor that allows higher performers to retain and recall information that enhances their performance."[42] Finally, the quality of work performance varied with heartbeat as higher performers experienced "more regular heart beat rates during the week particularly weekdays."[43] The study's passive sensors, therefore, found close links between workplace performance and weekend phone use, sleep in one's own bed, and the rhythm of one's own heartbeat—personal details long considered beyond the relevance of an employer's attention. The researchers saw their study as only the beginning, noting their work "opens the way to new forms of passive objective assessment and feedback to workers to potentially provide week-by-week or quarter-by-quarter guidance in the workplace."[44]

III. FOURTH AMENDMENT CONCERNS CREATED BY EMPLOYERS' PASSIVE MONITORING OF WORKERS' PHONE USAGE, MOVEMENTS, AND PHYSIOLOGICAL DATA

A. Over the Long Term, Widespread Employee Acceptance of Passive Monitoring Could Lessen Privacy Expectations in Shared Information, Undermining Claims that Police Commit a Fourth Amendment Search by Accessing Employer Data

Law enforcement, in its ongoing effort to improve its investigations, could find an employer's accumulation of passive monitoring data a ready tool aiding its crime detection. Any inquiry into privacy issues of passive monitoring begins with *Katz v. United States*, the seminal case providing the Court's most recent definition of a Fourth Amendment "search."[45] In *Katz*, Federal Bureau of Investigation (FBI) agents attached an electronic listening device to the outside of a public telephone booth to record Katz's voice as he illegally transmitted "wagering information."[46] In considering whether the FBI's eavesdropping implicated Fourth Amendment privacy rights, the Court recognized that when Katz occupied the phone booth, shut its door, and paid his toll, he was "surely entitled to assume that the words he utter[ed] into the mouthpiece [would] not be broadcast to the world."[47] Therefore, the FBI's eavesdropping on Katz's call "violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[48]

---

[42] *Id*.
[43] *Id*. at 20.
[44] *Id*. at 21. Study coauthor Pino Audia—a professor of management and organizations at Dartmouth's Tuck School of Business—suggested: "Passive sensors, which are the heart of the mobile sensing system used in this research, promise to replace the surveys that have long been the primary source of data to identify key correlates of high and low performers." *Science Daily*, *supra* note 2.
[45] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Note, that the Court, in *United States v. Jones*, resurrected the "common law trespass" definition of a Fourth Amendment search described in the prohibition era case, *Olmstead v. United States*. United States v. Jones, 565 U.S. 400, 405 (2012); Olmstead v. United States, 277 U.S. 438, 464 (1928). The *Olmstead/Jones* physical intrusion test, however, is beyond the scope of this Article.
[46] *Id*. at 348.
[47] *Id*. at 352.
[48] *Id*. at 353.

Justice Harlan, in his concurrence, provided an explanation of what is now recognized[49] as the Court's definition of a Fourth Amendment search: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[50] Justice Harlan further noted, "a man's home is, for most purposes, a place where he expects privacy."[51] In contrast, "objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."[52] Justice Harlan's reference to exposure of items to plain view, along with the Court's warning that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection,"[53] demonstrate that *Katz* crafted a double-edged sword. *Katz* extended Fourth Amendment privacy to places outside the home, intoning, "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[54] At the same time, however, *Katz* refused to extend privacy protection to such a traditionally private area as the home if the homeowner's own actions exposed that locale to the public by plain view.[55] The Court thus placed part of the privacy determination in the hands of the individual—if one wishes something to be private from government scrutiny, one must avoid conduct that could expose information to others, even civilians.

The significance of *Katz's* inclusion in its "search" definition of the impact of individual conduct on privacy was dramatically demonstrated in *United States v. Miller*.[56] In *Miller*, the defendant was charged with having an unregistered still, possessing 175 gallons of whiskey, and failing to pay the whiskey tax.[57] Miller moved to suppress bank records that the government obtained in violation of the Fourth Amendment.[58] The Court found "no legitimate expectation of privacy" in the contents of Miller's banking records because Miller's checks, deposit slips, and other records were "not confidential communications but negotiable instruments to be used in commercial transactions" and thus not protected by the Fourth Amendment.[59] Accordingly, the Court found Miller's argument that he only gave the banks documents "for a limited purpose" unconvincing because all of the documents contained "only information voluntarily conveyed to the

[49] The Court in *Smith v. Maryland*, 442 U.S. 735, 740 (1979) noted, "Consistently with *Katz*, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action." *Smith* further specified, "This inquiry, as Mr. Justice Harlan aptly noted in his *Katz* concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy...The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as reasonable.'" *Id*.

[50] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[51] *Id*.

[52] *Id*.

[53] *Id*. at 351.

[54] *Id*. at 359.

[55] *Id*. at 351 (Holding that "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.")

[56] United States v. Miller, 425 U.S. 435 (1976).

[57] *Id*. at 436.

[58] *Id*. at 436-37.

[59] *Id*.

banks and exposed to their employees in the ordinary course of business."[60] *Miller* emphasized the individual's own conduct in undermining the reasonableness of his assertion of privacy expectations, noting that each depositor "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[61] The Court thereby created what has become known as the "third party doctrine,"[62] which dictates that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[63]

The Court reaffirmed the third party doctrine in *Smith v. Maryland*, where police investigated a man who made "threatening and obscene phone calls" to a victim he previously robbed.[64] By tracing the license plate of Smith's vehicle, officers identified his phone number.[65] Police then used a pen register[66] to collect the numbers dialed from Smith's home phone,[67] leading to evidence used to convict him of robbery.[68] *Smith* raised the issue of whether use of a pen register constituted a Fourth Amendment search."[69] *Smith* ruled that the defendant had no reasonable expectation of privacy in the numbers he dialed from his phone, and therefore, that the police did not commit a "search" in using a pen register to collect those numbers.[70] The pen register, which only disclosed numbers of a phone call rather than the call's content, possessed only "limited capabilities" for privacy invasion.[71] The typical phone user understood that she must convey the numbers dialed to the phone company in order to complete the call.[72] As a result, the Court again declared that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[73] Smith, in using his phone, "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[74] He therefore assumed a risk that the phone company would reveal this information to police.[75] The act of sharing effectively destroyed reasonable privacy expectations.

The Court seriously reassessed the third party doctrine in *Carpenter v. United States*, involving law enforcement collection of cell-site location information (CSLI)[76] in an

[60] *Id*.
[61] *Id*. at 443.
[62] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[63] *Miller*, 425 U.S. at 443.
[64] Smith v. Maryland, 442 U.S. 735, 737 (1979).
[65] *Id*.
[66] *Id*. at 736, n. 1 (Noting that "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed.").
[67] *Id*. at 737.
[68] *Id*. at 737-38.
[69] *Id*. at 736.
[70] *Id*. at 745-46.
[71] *Id*. at 741-42.
[72] *Id*. at 743.
[73] *Id*. at 743-44.
[74] *Id*. at 744.
[75] *Id*.
[76] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

investigation of a series of robberies occurring in Michigan and Ohio.[77] CSLI exists because every smartphone constantly scans its area to obtain "the best signal, which generally comes from the closest cell site."[78] Smartphones "tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features."[79] Further, every time a phone connects to a cell site, "it generates a time-stamped record known as cell-site location information (CSLI)."[80] Federal prosecutors obtained a court order for providers MetroPCS and Sprint to hand over CSLI for Timothy Carpenter's cellphone.[81] The court orders[82] in *Carpenter* enabled the government to collect "12,898 location points cataloging Carpenter's movements—an average of 101 data points per day."[83] The CSLI "placed Carpenter's phone near four of the charged robberies" at the "exact time" of the robberies.[84] Carpenter was convicted and sentenced to "more than 100 years in prison."[85]

In *Carpenter,* the Court evaluated whether Government access to "historical cell phone records that provide a comprehensive chronicle of the user's past movements" constituted a Fourth Amendment search.[86] Troubled by the *comprehensiveness* of the information at issue,[87] the Court emphasized the ubiquity of phones, noting that phone accounts outnumbered people in the United States.[88] The *Carpenter* Court thus declared that it was confronting a "new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."[89] The fact that CSLI was "detailed, encyclopedic, and effortlessly compiled" was particularly alarming to the Court.[90] Specifically, CSLI gave an in-depth record of the holder's whereabouts over the course of several months, providing "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[91] CSLI not only expanded the government's ability to track someone in space, but it enabled police to "travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years."[92] Ultimately, the Court worried about leaving citizens "at the mercy of advancing technology," which could "encroach upon areas normally guarded from inquisitive eyes."[93] The *Carpenter* Court therefore held that the

[77] *Id*. at 2212.
[78] *Id*. at 2211.
[79] *Id*.
[80] *Id*. at 2212.
[81] Carpenter was one of the alleged robbers. *Id*.
[82] Federal Magistrate judges issued the orders in this case. *Id*. at 2212.
[83] *Id*.
[84] *Id*. at 2213.
[85] *Id*.
[86] *Id*. at 2211.
[87] *Carpenter* emphasized the comprehensiveness of the government intrusion, mentioning: "comprehensive chronicle," *Id*. at 2206; "comprehensive record," *Id*. at 221; "comprehensive dossier," *Id*. at 2220; and "comprehensive reach." *Id*. at 2223.
[88] "There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people." *Id*. at 2212.
[89] *Id*. at 2216.
[90] *Id*.
[91] *Id*. at 2217.
[92] *Id*. at 2218.
[93] *Id*. at 2214.

government, in collecting CSLI, "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[94]

The *Carpenter* Court's wariness of new technology that creates a "comprehensive chronicle" of a person's life could offer support to employees wishing to shield their passive monitoring data from police scrutiny.[95] Technology that detects each time an employee leaves her desk,[96] picks up her phone,[97] or experiences a change in heart rate,[98] readily qualifies as information that is "detailed and encyclopedic"[99] and as an "all-encompassing record of the holder's whereabouts."[100]

Moreover, the ease of employer data collection from "continuous sensing tools" would reasonably trouble a Court concerned about the effortlessness of information gathering from CSLI.[101] Employers' ability to store data for years or even decades to use in promotion and pay raise decisions would likely offend the Court that was troubled by the storage of CSLI data for only five years.[102] Indeed, the employer's intrusion here is even greater than that posed by CSLI because wearables give information about sleep, thus providing a window into employees' bedrooms.[103] Further, wearables probe an employees' heart rate, a physiological function magnitudes more personal than information about one's location on a public street.[104] The passive monitoring data thus provides clues to a worker's "emotional and behavioral well-being" and psychological states, intrusions beyond anything possible with CSLI.[105] Finally, wearables count both steps taken and calories burned, revealing evidence of physical fitness and weight, which can be quite sensitive subjects. Thus, confronted with the combined scrutiny from wearables, phones, and beacons of employees, courts could rightly find an invasion of reasonable privacy expectations, as the Supreme Court did in *Carpenter*.[106]

Carpenter's defense of one's right to privacy from passive monitoring, however, must contend with other third party cases that define the boundaries of reasonable privacy expectations more broadly.[107] Specifically, *Katz* warned that the Fourth Amendment did not protect information knowingly exposed to the public.[108] Employees who submit to wearables, phone applications, and beacons could be said to have reduced their own privacy by choosing to display data to the "plain view" of outsiders.[109] Further, under *Miller*, employees' movements, phone usage, heart rate, and sleep could be labeled as "the

[94] *Id*. at 2219.
[95] *Id*. at 2211.
[96] *See* Mirjafari, *supra* note 4 at 8.
[97] *Id*. at 18.
[98] *Id*. at 20.
[99] *See Carpenter*, 138 S. Ct. at 2216.
[100] *Id*. at 2217.
[101] *Id*. at 2216.
[102] *Carpenter* warned of CSLI, "With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense." *Id*. at 2218.
[103] *See* Mirjafari, *supra* note 4, at 20.
[104] *Id*.; *Carpenter* involved government intrusions "in an area accessible to the public." *See Carpenter*, 138 S. Ct. at 2217.
[105] *Science Daily*, *supra* note 2; Mirjafari, *supra* note 4, at 8.
[106] *Carpenter*, 138 S. Ct. at 2219.
[107] *Katz*, 389 U.S. at 351; *Miller*, 425 U.S. at 442.
[108] *Id*. at 351.
[109] *Id*. at 361 (Harlan, J., concurring).

business records" of the employer, who has established a "substantial stake in their continued availability and acceptance" as evidence justifying employment decisions.[110] Further, any employee who argues that she gave access to this personal data only for the "limited purpose" of performance assessment would be offering a contention already rejected by the Court.[111] Thus, *Miller* would not protect employees who "voluntarily conveyed" and "exposed" such personal data to their employers in "the ordinary course of business."[112] *Miller* suggests that employees took a "risk" in revealing their data to their employers, since the data could "be conveyed by [the employer] to the Government."[113]

The answer to these arguments resides in the dramatic advancement of technology. *Carpenter* found the traditional third party arguments unconvincing because new technology, such as CSLI, was simply so "qualitatively different" from the relatively simple banking and pen register technology considered in *Smith* and *Miller*[114] that these cases offered little guidance in the 21st century. Third party doctrine thus failed to "contend with the seismic shifts in digital technology."[115]

Moreover, third party doctrine, premised on actively opting in to the sharing of information, does not adequately address voluntariness. The *Carpenter* Court noted that the third party doctrine was based on the reduced privacy expectations caused by knowingly sharing information.[116] This "voluntary exposure" rationale, however, did not "hold up" for CSLI because this data was "not truly 'shared' as one normally understands the term."[117] Since cell phones were "indispensable to participation in modern society" and collection of CSLI occurred "without any affirmative act on the part of the user beyond powering up," *Carpenter* concluded "in no meaningful sense" did a phone user voluntarily assume the risk of "turning over a comprehensive dossier of his physical movements."[118] Similarly, monitored employees do not consciously upload the information for their employers because all data is passively collected.[119] An employee, like a cellphone user, is not truly sharing this information in an active manner as Miller did when writing a check or Smith did in dialing a number.

However, in any workplace following the study design in *Differentiating Higher and Lower Job Performers*, the employee would make an initial conscious choice to share his data with his employer, opting into a program and receiving compensation for participating. This decision to opt in could cause the Court to find that the employee triggered the Fourth Amendment's traditional third party doctrine of *Miller* and *Smith*, rather than the exception in *Carpenter*. Such employees opting into information-sharing schemes create difficult issues about the true nature of voluntariness.

---

[110] *Miller*, 425 U.S. at 440.
[111] *Miller*, 425 U.S. at 442.
[112] *Id*.
[113] *Id*.
[114] *Carpenter*, 138 S. Ct. at 2216. *Carpenter* ruled, "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id*. at 2217.
[115] *Id*. at 2219.
[116] *Id*.
[117] *Id*. at 2220.
[118] *Id*.
[119] Mirjafari, supra note 4 at 8.

The specter of employees torn by the choice between privacy and compensation is already playing out in work environments today. United Parcel Service (UPS) gathers data on its employees every day by using a black box in its trucks to record a driver's activity "to the second when he opens or closes the door behind him, buckles his seat belt and [] starts the truck."[120] UPS then analyzes these measurements to improve productivity.[121] This monitoring affects UPS' bottom line, as "[j]ust one minute per driver per day over the course of a year adds up to $14.5 million."[122] Since UPS can now improve a driver's delivery rate from 90 to 120 packages a day, the company views data as "about as important as the package."[123] The smallest movements do not escape notice. For instance, upon noticing that opening drivers' doors with a key slowed the drivers down, UPS switched to key fobs.[124] As one driver acknowledged, the tracking "feel[s] like big brother."[125] The driver reasoned, however, that he could not allow himself to perceive the monitoring as a personal attack because if he did, his frustration could lead him to not "even want to do it anymore."[126] The pain of intrusion on driver's privacy is superseded, however, by financial incentive; UPS drivers, are "the highest paid in the business."[127] Thus, the practical realities of making a living have required drivers to trade privacy for compensation. Do UPS drivers calmly and fully consider the long view when accepting monitoring, or do they only consider the next rent payment? Have drivers, in choosing to accept monitoring, thought about and assumed the risk that UPS might choose to share their information with law enforcement? In short, can it truly be said that UPS drivers voluntarily chose to expose this information to a third party?

If drivers have become inured to sharing their movements, other employees might reasonably become accustomed to sharing more personal data, such as phone use, sleep in the bedroom, and the beating of one's own heart. These shifts in attitudes could significantly affect Fourth Amendment privacy rights. The *Carpenter* Court might shudder at the thought of compiling a comprehensive chronicle of a person's movements; but, UPS drivers could see such a prospect as old news.[128] Thus, *Carpenter's* effectiveness in promoting the rights of passively monitored employees could, as time passes, become the slenderest of reeds upon which to lean, given the consent given by employees for such monitoring.

Employees' inurement to privacy invasion leads to another concern: any assertion of a right to privacy from passive monitoring would need to account for the ever evolving, and perhaps dissipating, nature of *Katz's* reasonable privacy expectations in the wake of daily advancing technological intrusions. Society's recognition of what constitutes a reasonable privacy expectation will inevitably evolve over time. Although *Carpenter* declared "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of

[120] *Id*.
[121] *Id*.
[122] *Id*.
[123] *Id*.
[124] *Id*.
[125] *Id*.
[126] *Id*.
[127] *Id*.
[128] *Carpenter*, 138 S. Ct. at 2211.

science' does not erode Fourth Amendment protections,"[129] the Court's ability to protect privacy from technology's inroads on society's reasonable expectation of privacy is alarmingly inconstant. The very process of scientific advancement could numb the populace to the intrusiveness of ever more ubiquitous technology.

Society's incremental acceptance of the erosion of privacy is demonstrated by one of the most common law enforcement intrusions, the *Terry* stop and frisk, recognized by the Court in *Terry v. Ohio*.[130] In 1968, when the *Terry* Court considered a pat down frisk of a detainee, it did not minimize the severity of the government intrusion, instead noting that the "careful exploration of the outer surfaces of a person's clothing all over his or her body in an attempt to find weapons" was "a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly."[131] Justice Scalia even questioned "whether the fiercely proud men who adopted our Fourth Amendment would have allowed themselves to be subjected, on mere *suspicion* of being armed and dangerous, to such indignity."[132] With quickly advancing technology, however, electronic frisks for weapons at airports and large venues are now seen as only a hassle rather than a "petty indignity," a label *Terry* dismissed as inadequately describing the intrusive nature of its frisk.[133] Societal acceptance of electronic frisks is now unremarkable, even though the practice is arguably more intrusive than a pat down on the street.[134] In fact, airport security scanners have found cysts and hernias, something not expected from a constable on patrol.[135]

The changing view of pat down frisks is not the only example of society's gradual acceptance of technologies used by authorities to gather personal information. In *Katz*, the Court deemed electronic eavesdropping on only one side of a phone conversation to be a Fourth Amendment search.[136] Now, however, people are accustomed to overhearing one side of a cell phone call, whether in a restaurant, a waiting room, or on the sidewalk. Further, "[c]ookies track our every move online"[137]—whether we are visiting sites regarding medical conditions, politics, or religion—with little reaction from the public other than a shrug of futility.

The Court considered whether government use of a thermal imager to detect heat from inside a home in an effort to detect marijuana cultivation constituted a Fourth Amendment search in *Kyllo v. United States*.[138] The *Kyllo* Court established a "firm" and "bright" rule that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical

---

[129] *Id.* at 2223.
[130] Terry v. Ohio, 392 U.S. 1, 29–30 (1968).
[131] *Id*. at 16, 17.
[132] Minnesota v. Dickerson, 508 U.S. 366, 381 (1993) (Scalia, J., concurring).
[133] *Terry*, 392 U.S. at 17.
[134] Warren R, Heymann, M.D., A Cyst Misinterpreted on Airport Scan as Security Threat, *JAMA Dermatol ogy*. 2016;152(12):1388. doi:10.1001/jamadermatol.2016.3329, https://jamanetwork.com/journals/jamader matology/fullarticle/2547143.
[135] *Id*.
[136] *Katz*, 389 U.S. at 348, 353.
[137] Consumer Reports, *How and Why Retail Stores Are Spying on You: Many retailers are snooping more than ever*, SHOPSMART (March 2013), https://www.consumerreports.org/cro/2013/03/how-stores-spy-on-you/index.htm.
[138] Kyllo v. United States, 533 U.S. 27, 29 (2001).

intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[139] Today, *Kyllo's* privacy concerns sound almost quaint, as stores use sophisticated technology that, in one instance, told a father his daughter was pregnant before the daughter did.[140] Yet, people still shop. So, even though in the fifties, "The Adventures Ozzie and Harriet" show made television history by having Ozzie and Harriet "share a double bed," today, many might be unfazed that employees share sleep data with their employer even though it was gathered in the employee's bed.[141]

So, in the near term, pursuant to *Carpenter*, the Court would likely determine that individuals have a reasonable expectation of privacy from passive monitoring's creation of "a comprehensive dossier."[142] If past is prologue, however, in the future such passively collected data might become a societal norm no longer deemed deserving of privacy protections. Although the Court might maintain *Katz's* reasonable expectation of privacy definition, this test's reach will be so diminished that it no longer offers protection to employees.

B. Since the Court Has Previously Accepted the Needs of the Employer and Society as Reasons to Significantly Limit Employees' Reasonable Privacy Expectations, the Court Could Allow Passive Monitoring of Employees

Precedent assessing the Fourth Amendment privacy of employees offers additional insight into protections for workers' privacy from police pursuit of passive monitoring data. Over a half-century ago, in *Mancusi v. Deforte*, the Court applied the *Katz* test in weighing the privacy expectations of a Teamsters Union official.[143] In *Mancusi*, a grand jury indicted Frank DeForte "on charges of conspiracy, coercion, and extortion" for forcing juke box owners to pay him tribute.[144] State agents committed a warrantless search of an office DeForte shared with other union officials.[145] The Court considered whether DeForte had "a reasonable expectation of freedom from governmental intrusion" in the union office.[146] *Mancusi* noted that even though DeForte had a large room for an office and shared this space with others, he could still affect the reasonableness of his own privacy expectations.[147] Since DeForte spent considerable time in his office and had "custody" of

---

[139] *Id*. at 40.

[140] Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, FORBES (February 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#25c9e6e66686. The article noted, "Every time you go shopping, you share intimate details about your consumption patterns with retailers." Such sharing of information undermines every shopper's reasonable privacy expectations, as previously discussed in the third-party precedent in Part II above. More to the point, despite the intrusiveness of the store's technology, shoppers still choose to do business with Target.

[141] Roger K. Miller, *The First Family of TV*, LOS ANGELES TIMES (October 3, 2002), https://www.latimes.com/archives/la-xpm-2002-oct-03-wk-miller3-story.html.

[142] *Carpenter*, 138 S. Ct. at 2220.

[143] Mancusi v. DeForte, 392 U.S. 364, 365 (1968).

[144] *Id*.

[145] *Id.*

[146] *Id*. at 368. Although *Mancusi* framed the issue in terms of standing by inquiring, "whether DeForte has Fourth Amendment standing to object to the seizure of the records," it answered this query by applying *Katz's* reasonable expectation of privacy test. *Id*. at 367-368.

[147] *Id*.

his papers, the *Mancusi* Court ruled that he had a Fourth Amendment right to contest the invasion.[148] DeForte enjoyed privacy because he could "expect that he would not be disturbed except by personal or business invitees, and that records would not be taken except with his permission or that of his union superiors."[149] When assessing the constitutional impact of individuals sharing access to information, the Court in *Mancusi* reasoned quite differently for employee expectations than it did for the third parties in *Miller* and *Smith*. Specifically, DeForte's sharing of an office did not fundamentally change his privacy because he could have reasonably expected that only certain persons would enter the office and that records would only be accessed with permission.[150] In contrast, the Court rejected such reasonable assumptions in *Miller* and *Smith* due to the exposure of information to third parties.[151]

Nearly two decades later, the Court considered the Fourth Amendment rights of employees in *O'Connor v. Ortega*, a civil case involving a psychiatrist contesting his dismissal from a state hospital for sexual harassment and other improprieties.[152] The psychiatrist's superiors made a thorough search of his office, seizing "several items from Dr. Ortega's desk and file cabinets, including a Valentine's Day card, a photograph, and a book of poetry all sent to Dr. Ortega by a former resident physician."[153] The Court considered whether Dr. Ortega, "a public employee, had a reasonable expectation of privacy in his office, desk, and file cabinets at his place of work."[154] *O'Connor* defined a "workplace" as including an area or item "related to work" and "generally within the employer's control."[155] Accordingly, the workplace involved tangible items and places, such as "hallways, cafeteria, offices, desks, and file cabinets."[156] The Court also discussed personal items an employee brought to the workplace. If an employee placed a personal item, such as a photograph, on a desk or bulletin board, the areas holding personal objects still remained "part of the workplace."[157] However, the items themselves, such as a "handbag or briefcase," could still remain outside the "workplace" designation even if they physically existed in a place of work.[158] Overall, employees had a reasonable expectation of privacy, even in the workplace context, against police intrusions into private areas such as personal offices.[159]

O'Connor warned that "actual office practices and procedures" could alter the "operational realities of the workplace" so significantly that employees' reasonable privacy expectations could be diminished.[160] For instance, employees' offices might be

---

[148] *Id*. at 368–69.
[149] *Id*. at 369.
[150] *Id*.
[151] *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 743–44.
[152] O'Connor v. Ortega, 480 U.S. 709, 712 (1987).
[153] *Id*. at 713.
[154] *Id*. at 711–12. The entry of the office and collection of items by the employer here had Fourth Amendment implications because Dr. Ortega's supervisors worked at a state hospital and thus were government actors. *Id*. at 714–15.
[155] *Id*. at 715.
[156] *Id*. at 716.
[157] *Id*.
[158] *O'Connor* noted, "Not everything that passes through the confines of the business address can be considered part of the workplace context." *Id*.
[159] *Id*.
[160] *Id*. at 717.

"continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits," thus eroding privacy expectations.[161] Indeed, "some government offices might be so open to fellow employees or the public that no expectation of privacy is reasonable."[162] Recognizing the "plethora" of workplace contexts, *O'Connor* cautioned that employee privacy assessments required case-by-case analyses.[163] The operational realities of *O'Connor's* workplace ultimately led the Court to accept that "Dr. Ortega had a reasonable expectation of privacy at least in his desk and file cabinets."[164]

O'Connor's application of the Fourth Amendment to the case, however, did not provide the employee all traditional Fourth Amendment protections. Since the searches were performed by government employers investigating worker malfeasance rather than by police pursuing evidence in a criminal investigation, the *O'Connor* Court deemed the case to be one of "special needs."[165] In such a case, the Court weighs "legitimate privacy interests of public employees in the private objects they bring to the workplace" against the government interests occasioned by "the realities of the workplace."[166] The needs of the public employer in completing "the government agency's work in a prompt and efficient manner" outweighed the privacy concerns of the employee who could "avoid exposing personal belongings at work by simply leaving them at home."[167] The weight given to the employer's special needs ultimately led the Court to forgo both the Fourth Amendment requirement that searches be supported by a warrant[168] and the mandate that searches be based on probable cause.[169]

As a special needs case, *O'Connor* might seem unhelpful in determining how the Court would handle a law enforcement search of employer records for evidence of a crime. *O'Connor*, however, is part of a collection of special needs cases in which the Court consistently ruled *against* providing the traditional protections of a warrant and probable cause to employees. In *Skinner v. Railway Labor Executives' Ass'n*, for instance, the Court considered whether Federal Railroad Administration (FRA) regulations, which either mandated or authorized the collection of biological samples from railroad employees, violated the Fourth Amendment.[170] One such FRA regulation[171] required that railroads

[161] *Id*.
[162] *Id*. at 718. *O'Connor* might have signaled a subtle diminution of employee privacy here, for the Court found repeated entries into a private office more corrosive to Fourth Amendment coverage than it did the continual sharing of DeForte's office in *Mancusi*. *Mancusi*, 392 U.S. at 369.
[163] *Id*. at 723, 718.
[164] *Id*. at 719.
[165] *Id*. at 720. *O'Connor* defined cases involving "special needs" as those involving interests "beyond the normal need for law enforcement," "making the warrant and probable-cause requirement impracticable." *Id*.
[166] *Id*. at 720, 719.
[167] *Id*. at 721, 725.
[168] *O'Connor* declared, "In our view, requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome." *Id*. at 720.
[169] *O'Connor* concluded, "In sum, we conclude that the special needs, beyond the normal need for law enforcement make the ... probable-cause requirement impracticable." *Id*. at 725.
[170] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 609–12 (1989).
[171] This regulation, Subpart C, was entitled, "Post–Accident Toxicological Testing," *Id*. at 609.

collect blood and urine samples from employees involved in any recent railroad accident.[172] *Skinner* held that compelled blood alcohol tests amounted to Fourth Amendment searches.[173] Likewise, since there existed "few activities in our society more personal or private than the passing of urine," *Skinner* recognized that urine tests intruded upon reasonable expectations of privacy."[174] Importantly, however, despite the sensitive nature of the intrusions involved, the government's special need in ensuring railroad safety outweighed the intrusions of employee privacy.[175]

While recognizing that the toxicological testing of employees could be viewed as significant in other situations, the Court found railroads involved diminished privacy expectations.[176] Even though the Court noted that the passing of urine is so private that most persons "describe it by euphemisms if they talk about it at all,"[177] *Skinner* equated the privacy intrusion associated with the FRA urine collection akin to an annual physical.[178] Further, the Court found a blood test's intrusion insignificant since such "tests are a commonplace in these days of periodic physical examinations."[179] Finally, the Court found the employees, by choosing to participate in the regulated industry of railroads, diminished their own privacy expectations.[180] The employees' privacy rights were thus so diminished, in comparison to the needs of the employers, that *Skinner* upheld the biological collections without requiring a warrant, probable cause, or even reasonable suspicion.[181]

United States Customs Service employees in *National Treasury Employees Union v. Von Raab* fared little better than the railroad workers in *Skinner*.[182] In *Von Raab*, agents were subject to drug testing when seeking Customs Service positions requiring the carrying of a firearm or directly involving drug interdiction.[183] Invoking "special government needs," the Court declared, "it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[184] Accordingly, the "operational realities of the workplace" might "render entirely reasonable certain work-related intrusions by supervisors and co-workers that might be viewed as unreasonable in other contexts."[185] In this context, customs employees working directly with drugs and guns had lessened privacy expectations.[186] The agents' privacy interests therefore did not outweigh the government's interests in their "fitness and probity."[187] The

[172] *Id*.
[173] *Id*. at 616.
[174] *Id*. at 617.
[175] *Id*. at 619–620, 628.
[176] *Id*. at 628.
[177] *Id*. at 617.
[178] *Id*. at 626-627.
[179] *Id*. at 625.
[180] *Id*. at 627.
[181] *Id*. at 624, 633.
[182] National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).
[183] *Id*. at 660–61, 667–77.
[184] *Id*. at 665–66.
[185] *Id*. at 671.
[186] *Id*. at 672.
[187] *Id*. at 672, 679. Remarkably, the Court refused to find diminished privacy expectations for workers subjected to biological testing in *Chandler v. Miller*. Chandler v. Miller, 520 U.S. 305 (1997). This case, in dealing with drug testing of officials, professionals, and supervisors rather than traditional workers, is the

warrantless and suspicionless biological testing was thus reasonable under the Fourth Amendment.[188]

Special needs precedent is not alone in restricting the Fourth Amendment rights of employees. The Court has also used employees' own choices to limit their Fourth Amendment rights against seizure of the person.[189] In *I.N.S. v. Delgado*, the Court considered the Fourth Amendment implications of the Immigration and Naturalization Service's (INS) use of "factory surveys" to determine if workers at three garment factories were undocumented.[190] To carry out the surveys, some INS agents would position "themselves near the buildings' exits" while others "dispersed throughout the factory to question most, but not all, employees at their work stations."[191] The INS agents, wearing badges and armed with weapons and walkie-talkies, asked workers about their

---

exception that proves the rule that the Court has shown little interest in providing the traditional protections of a warrant and probable cause to employees. *See* George M. Dery III, *Are Politicians More Deserving of Privacy than Schoolchildren? How Chandler v. Miller Exposed the Absurdities of Fourth Amendment "Special Needs" Balancing*, 40 ARIZONA L. REV. 73 (1998). In *Chandler*, Georgia passed legislation mandating persons running for certain state offices "certify that they have taken a drug test and that the test result was negative." *Chandler*, 520 U.S. at 308. The state officials subject to the drug certification were:

> the Governor, Lieutenant Governor, Secretary of State, Attorney General, State School Superintendent, Commissioner of Insurance, Commissioner of Agriculture, Commissioner of Labor, Justices of the Supreme Court, Judges of the Court of Appeals, judges of the superior courts, district attorneys, members of the General Assembly, and members of the Public Service Commission.

Id. at 309–10. Libertarian Party nominees Chandler, Harris, and Walker sued in federal court contending the mandatory drug tests violated the Fourth Amendment. *Id.* at 310. The District Court "denied petitioners' motion for a preliminary injunction" and the Eleventh Circuit Court of Appeals affirmed, noting the significant societal interests involved:

> [t]he people of Georgia place in the trust of their elected officials ... their liberty, their safety, their economic well-being, [and] ultimate responsibility for law enforcement." Consequently, "those vested with the highest executive authority to make public policy in general and frequently to supervise Georgia's drug interdiction efforts in particular must be persons appreciative of the perils of drug use.

Id. at 311. To assess the "special needs" being "alleged" in the case, *Chandler* noted, "courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties." *Id*. at 314. Declaring, "the proffered special need for drug testing must be substantial—important enough to override the individual's acknowledged privacy interest," *Chandler* found Georgia failed to meet this standard. *Id*. at 318. On the other side of the special needs balance, when weighing the privacy interests of candidates for state office, *Chandler* noted the lack of need to invade official's privacy because, "Candidates for public office…are subject to relentless scrutiny—by their peers, the public, and the press. Their day-to-day conduct attracts attention notably beyond the norm in ordinary work environments." *Id*. at 321. In prior Court cases, such an argument, that those subject to the intrusion of biological testing have already exposed themselves to great scrutiny, would prove that the workers have chosen to lessen the reasonableness of their own privacy expectations rather than to establish the lack of government interests in the intrusion. *Skinner*, 489 U.S. at 627. The greatest difference between *Chandler* and earlier drug testing cases was not mentioned by the Court—in *Chandler*, the government sought to have those seeking high office, including judges, submit to a privacy invasion. *Chandler*, 520 U.S. at 309–310. The Court, after weighing the interests, determined that the suspicionless candidate drug tests, "(h)owever well meaning," did not satisfy Fourth Amendment reasonableness. *Id*. at 322.

[188] *Von Raab*, 489 U.S. at 672.

[189] I.N.S. v. Delgado, 466 U.S. 210 (1984). *Delgado* was not a "special needs" case. In fact, the INS had obtained warrants for its investigations in this case. *Id*. at 212.

[190] *Id*. at 212.

[191] *Id*.

citizenship.[192] Yet, "employees continued with their work and were free to walk around within the factory."[193] As a result, *Delgado* found that "these factory surveys did not result in the seizure of the entire work forces."[194] Specifically, the Court rejected the contention that placement of INS agents created a seizure of all workers at the factories because employees' "freedom to move about" at work is meaningfully restricted by their own "voluntary obligations to their employers" rather than "by the actions of law enforcement officials."[195] Once again, an employee could undermine her own Fourth Amendment claim by personal choices made in the course of work.

The Court's early case, *Mancusi*, provides a basis for considering employees' privacy against police collection of passive monitoring data. Fifty years ago, the Court viewed employees' rights as relatively robust, for DeForte could overcome the limits to his privacy caused by sharing.[196] DeForte could preserve his privacy by using time and exercising possession—he won back his privacy by spending a "considerable amount of time" in the shared office and by maintaining "custody" of his papers.[197] Further, he could reasonably expect fellow employees to respect his privacy since they were expected to forgo touching his items unless permitted by supervisors.[198] The Court made no mention that employees assume any risk of others sharing items or information with police.[199] If *Mancusi* was the only case addressing employees' Fourth Amendment rights, workers might expect to maintain privacy from police requests for data regarding location, phone usage, and emotional states implied from heart rate. If an employee may reasonably expect privacy from police intrusion into an office, she certainly should reasonably assume privacy from official intrusion into a private cell phone located in the office or in data collected not from the office, but from the bedroom. An employee's sharing of such data would not lead to diminished privacy expectations, in light of the shared nature of DeForte's office. However, technological advances and workplace norms have affected employees' lives in the half-century since the Court decided *Mancusi*.

O'Connor, which defined the "boundaries of the workplace context" nineteen years after *Mancusi*, offers workers less assurance of privacy in passive monitoring data.[200] *O'Connor* might be a less than perfect fit, however, considering its 1980s context, where the workplace involved tangible office spaces separate from the home, as opposed to digital data.[201] *O'Connor*, therefore, spoke of a workplace exclusively "related to work" and "within the employer's control," notions that dissolve when considering employees increasingly work from home with digital devices.[202] Moreover, the crucial point of the *Differentiating Higher and Lower Job Performers* study is that behavior seemingly unconnected to work, whether phone use on weekends, mobility on weekends, deep sleep in one's own bedroom, or heart rate in one's own body, are now directly "related to work"

[192] *Id*.
[193] *Id*. at 213.
[194] *Id*. at 212.
[195] *Id*. at 218.
[196] *Mancusi*, 392 U.S. at 368.
[197] *Id*. at 368-93.
[198] *Id*. at 369.
[199] *Miller*, 425 U.S. at 443.
[200] *O'Connor*, 480 U.S. at 715.
[201] *Id*. at 716.
[202] *Id*. at 715.

since activities affect worker performance.[203] While an employee's phone usage, movements, sleep, and heart rate are not directly within the employer's control, via constant monitoring, they are within a supervisor's continual view. The practical purpose of measuring such behavior is to modify it for optimum performance. Employers might turn job reviews into coaching sessions encouraging more exercise on the weekends, avoidance of alcohol that can impair sleep, and earlier bedtimes. The *Differentiating Higher and Lower Job Performers* study's results hinted at such prodding, as the researchers meticulously checked the "compliance rate for each participant" for each of 48 time slots in a 24-hour day,[204] with the study authors finding it "useful" to inform participants of any "problems with their compliance rates."[205] This was bolstered by a carrot/stick approach because employees were compensated according to compliance rates in wearing the devices.[206] *O'Connor*—decided well before the digital revolution—could not have predicted such employer scrutiny of employees, let alone offer specific rules for this passive monitoring.

A further disconnect between *O'Connor* and workers today involves the personal items employees bring to the workplace. *O'Connor* took care to protect the privacy of the contents of items employees brought to their jobsites, such as briefcases.[207] Today, it is these very items—cell phones, tablets, and wearables—which intrude on employee privacy. While *O'Connor* suggested to employees that they could avoid privacy intrusions by simply leaving personal items at home, [208] the Court recently recognized the practical impossibility of such a suggestion.[209]

Despite its limitations, *O'Connor* may provide some understanding about the Court's views concerning employee monitoring. The most helpful guidance for assessing the privacy of passively monitored data comes from *O'Connor's* general admonition to consider "actual office practices and procedures" to measure the "operational realities of the workplace."[210] In a formal sense, an office's "practices and procedures" are the written and agreed-upon guidelines directly addressing employee privacy policies. Such procedures, however, form only a part of the reasonable expectation of privacy analysis, which considers "all the circumstances."[211] The actual "operational realities of the workplace," which play out daily, could undermine written employment policies.[212] Employees who need a pay increase for financial stability, are ambitious for the next promotion, or fear losing their jobs in a competitive workplace might be vulnerable to employer suggestions that money, advancement, and job security could be bolstered by "voluntary" participation in a passive monitoring program. Concern about the prospect of not being perceived as a team player could increase pressure to opt in. Indeed, teambuilding

[203] Mirjafari, *supra* note 4, at 18-20.
[204] *Id*. at 6.
[205] *Id*. at 9.
[206] *Id*.
[207] *O'Connor*, 480 U.S. at 716.
[208] *Id*. at 725.
[209] The Court has now deemed the cell phone as "almost a 'feature of human anatomy.'" *Carpenter*, 138 S. Ct. at 2218. *Carpenter* noted, "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Id*.
[210] *O'Connor*, 480 U.S. at 717.
[211] *Mancusi*, 392 U.S. at 368.
[212] *O'Connor*, 480 U.S. at 717.

itself is an example of a corporate practice that could significantly alter a workplace's operational realities.

Teambuilding has been called "the most important investment you can make for your people" because it boosts "the bottom line.[213] Employers therefore try to mold workers into teams through a dizzying variety of exercises: holding a "daily huddle,"[214] "great white shark-spotting," entry into a "Spy School Program" complete with crossbow-shooting, having a lesson to learn how to survive a plane crash,[215] employee trivia games, creating one's own job title, and escape rooms.[216] It is not enough to build a team; teamwork must be "baked" into a company's culture.[217] Team building can exploit game theory, which "leverages people's natural tendencies to compete" and "strive for status."[218] Employers could encourage employees to opt into teams of workers who compete against each other to improve their teams' numbers on company-appropriate phone use, exercise and movement metrics, hours and stages of sleep, and even regularity of heart rates. Employers could even incentivize "compliance" with passive monitoring by rewarding those teams whose members shared the most information during a 48-time slot 24-hour day.[219] At an early stage of monitoring, any employee concerned about preserving her own privacy need simply not join, and consequently only lose out on the "extras" earned by more "dedicated" employees.[220] If participation, with its monetary rewards, became the norm, however, the few holdouts would find themselves in an "operational reality" of routine employee disclosure of information and therefore could no longer expect privacy to be the norm at such a business.

The workplaces operating with large buy-ins by employees focused on raises or promotions, in stripping employees of privacy, would begin to resemble those employing railroad workers in *Skinner* or United States Customs agents in *Von Raab*.[221] When

---

[213] Brian Scudamore, *Why Team Building Is the Most Important Investment You'll Make*, FORBES (March 9, 2016), https://www.forbes.com/sites/brianscudamore/2016/03/09/why-team-building-is-the-most-important-investment-youll-make/#2db6eafc617f.

[214] *Id*.

[215] Kenneth Kriesnoski, *The Wildest, weirdest corporate team-building trip ideas*, CNBC (July 26, 2017), https://www.cnbc.com/2017/07/26/the-wildest-weirdest-corporate-team-building-trip-ideas.html.

[216] Expert Panel, Forbes Human Resources Council, *12 Surprisingly Effective Yet Unconventional Team-Building Exercises*, FORBES (December 30, 2019) https://www.forbes.com/sites/forbeshumanresourcescouncil/2019/12/30/12-surprisingly-effective-yet-unconventional-team-building-exercises/.

[217] Michigan State University, *Baking Teamwork Into the Company Culture*, MICHIGAN STATE UNIVERSITY (July 12, 2019), https://www.michiganstateuniversityonline.com/resources/leadership/baking-teamwork-into-the-company-culture/.

[218] *Id*.

[219] Mirjafari, *supra* note 4 at 6, 9.

[220] This choice could be analogous to *O'Connor's* suggestion that employees wishing to "avoid exposing personal belongings at work" could achieve this privacy by "simply leaving them at home." 480 U.S. at 725.

[221] At Amazon, employees already experience intrusions on privacy akin to those in *Skinner*. Nina Godlewski, *Amazon Working Conditions: Urinating in Trash Cans, Shamed to Work Injured, List of Employee Complaints*, NEWSWEEK September 12, 2018 According to *Newsweek*, employees have reported lacking "time for bathroom breaks" and have resorted to "urinating in bottles and trashcans." *Id*. One employee is suing Amazon for firing him for taking too many bathroom breaks. The public has heard such

assessing privacy, context is crucial because the "operational realities of the workplace" could recast intrusions "unreasonable in other contexts" as "entirely reasonable" for "certain work-related intrusions."[222] If the company culture prods employees to share specifics about sleep or phone use, whether in the context of team building or as part of a competition for financial incentives, such collective disclosure could change the work landscape. This could ultimately lead the Court to find access to such information "entirely reasonable,"[223] despite the intimate nature of the information. Since *Skinner* already allowed the collection of blood and urine, passive monitoring to gather sleep and heart rate data could progressively appear to be within the corporate norm. Pursuant to *Skinner*, the Court might even blame the employee for her diminished privacy expectations by reminding the worker that she chose to participate by taking the job (or in opting into the monitoring program) in the first place.[224] The Court has used employees' choices to limit not only their Fourth Amendment rights against unreasonable searches, but also against unreasonable seizures. In *Delgado*, the Court refused to find that garment employees had been seized by federal agents standing at the factory exits because these workers voluntarily chose to meaningfully limit their own movement by agreeing to stay at the factory while working.[225] These workers' decisions, probably taken without much reflection beyond wishing to have a job, had dramatic legal consequences: employees found no Fourth Amendment protection from INS agents standing at the factory door.[226]

Employee Fourth Amendment rights have devolved considerably since DeForte vindicated his right to privacy in his shared office in 1968 in *Mancusi*.[227] While the Court could find that employees have a reasonable expectation of privacy in the data gathered by passive monitoring, such a ruling is in no way guaranteed. The Court could instead apply *O'Connor's* definition of a "workplace" to determine that data about an employee's emotional state, nightly sleep, or weekend activity relevant to productivity on the job is now appropriately "related to work."[228] Since such activities or attributes directly affect a company's bottom line, they could be deemed "generally within the employer's control."[229] *O'Connor's* "operational realities of the workplace" test, applied on a case-by-case basis, takes on a fluid quality that changes with each job and thus provides scant hope of permanent protection.[230] The one constant seems to be that the Court, whether following *O'Connor*, *Skinner*, or *Delgado*, will hold an employee to the decision she makes, whether in bringing something personal to work[231] or in taking the job in the first place.[232]

---

complaints because such conditions are not the norm and therefore newsworthy. However, it is telling that employees remain at these jobs despite such conditions, for $15 an hour. *Id*.

[222] *Von Raab*, 489 U.S. at 671.

[223] *Id*.

[224] *Skinner*, 489 U.S. at 627.

[225] *Delgado*, 466 U.S. at 218.

[226] *Id*.

[227] *Mancusi*, 392 U.S. at 368-69.

[228] *O'Connor*, 480 U.S. at 715.

[229] *Id*.

[230] *Id*. at 717-18.

[231] *Id*. at 725.

[232] *Skinner*, 489 U.S. at 627; *Delgado*, 466 U.S. at 218.

C. Employees' Tolerance of, or Submission to, Passive Monitoring, Could Make Employer Data Available to the Government Through Third Party Consent, Making any Fourth Amendment Search Reasonable

Even if an employee's choice to opt into passive collection of data does not trigger *Miller's* third party doctrine,[233] or so alter the operational realities of the workplace as to erode privacy expectations,[234] such a decision could have Fourth Amendment significance due to the third party consent exception to the warrant requirement. Specifically, the Court has ruled that law enforcement may intrude on a person's privacy, without a warrant, when it has gained consent from someone who possesses "common authority over or other sufficient relationship to the premises or effects sought to be inspected."[235] The Court recognized this "third party consent" principle in *United States v. Matlock*, a case involving investigation of a bank robbery by police.[236] Police officers arrested Matlock in the front yard of a home in which he had been living.[237] Rather than seeking consent from Matlock himself, officers placed Matlock in their squad car and went to the door of the house without him.[238] The Marshall family, of whom Gayle Graff was a daughter, was leasing the home.[239] Graff answered the door, and upon hearing from the officers that they were looking for money and a gun, consented to a search of the home, including the bedroom she "jointly occupied" with Matlock.[240] In their search of the room, officers recovered $4995 cash in a diaper bag.[241]

The search in *Matlock* raised the question of whether Graff, as a "third party," had the authority to give police consent to search a room she shared with Matlock.[242] The Court found the "common authority" Graff would need to provide such consent depended on the "relationship" she had to the area searched.[243] In particular, "common authority" was based "on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right."[244] Mutual access or joint use suggests that all inhabitants had "assumed the risk that one of their number might permit the common area

---

[233] *Miller*, 425 U.S. at 443.
[234] *O'Connor*, 480 U.S. at 717.
[235] United States v. Matlock, 415 U.S. 164, 171 (1974).
[236] *Id*. at 171, 166.
[237] *Id*. at 166.
[238] The Court in *Georgia v. Randolph* noted, "The defendant in [*Matlock*] was arrested in the yard of a house where he lived with a Mrs. Graff and several of her relatives, and was detained in a squad car parked nearby." Georgia v. Randolph, 547 U.S. 103, 109-110 (2006). *Matlock*, 415 U.S. at 166.
[239] *Matlock*, 415 U.S. at 166.
[240] *Id*.
[241] *Id*. at 166-67.
[242] *Matlock* framed the issue as follows, "The question now before us is whether the evidence presented by the United States with respect to the voluntary consent of a third party to search the living quarters of the respondent was legally sufficient to render the seized materials admissible in evidence at the respondent's criminal trial." *Id*. at 166.
[243] *Id*. at 171, 167.
[244] *Id*. at 171 n.7. *Matlock* further explained that the "common authority" to provide third party consent did "not rest upon the law of property, with its attendant historical and legal refinements." *Id*.

to be searched."[245] Thus, Matlock, in sharing a room with Graff, assumed a risk that Graff would open the door to others.[246]

The Court expanded on third party consent in *Georgia v. Randolph*, a case arising out of the troubled marriage of Scott and Janet Randolph.[247] Police responded to a domestic dispute where each spouse accused the other of substance abuse,[248] and Janet volunteered to police that there were "items of drug evidence" confirming Scott's use of cocaine in the home.[249] While Janet readily gave consent for police to search the house, Scott "unequivocally refused."[250] An officer then followed Janet into a bedroom in the home and recovered "a section of a drinking straw with a powdery residue," which was later offered as evidence of Scott's possession of cocaine.[251]

The Court in *Randolph* inquired whether a search is reasonable when police obtain "the permission of one occupant" even though the other occupant, "who later seeks to suppress the evidence, is present at the scene and expressly refuses to consent."[252] The Court held, "a physically present co-occupant's stated refusal to permit entry prevails, rendering the warrantless search unreasonable and invalid as to him,"[253] basing its holding on "widely shared social expectations."[254] The reasonableness of the officer's search of Scott's home was "in significant part a function of commonly held understanding about the authority that co-inhabitants may exercise in ways that affect each other's interests."[255]

Randolph applied its social expectations rule to a series of examples.[256] In *Matlock*, for instance, when Graff came to the door of her home "with a baby at her hip,"

> she shows that she belongs there, and that fact standing alone is enough to tell a law enforcement officer or any other visitor that if she occupies the place along with others, she probably lives there subject to the assumption tenants usually make about their common authority when they share quarters.[257]

By living with Graff, Matlock assumed a risk that Graff could admit a guest Matlock found obnoxious in his absence.[258] The *Randolph* Court offered the contrasting example of a

---

[245] *Id*.
[246] *Matlock* surmised, "the Government sustained its burden of proving by the preponderance of the evidence that Mrs. Graff's voluntary consent to search the east bedroom was legally sufficient to warrant admitting into evidence the $4,995 found in the diaper bag." *Id*. at 177.
[247] Georgia v. Randolph, 547 U.S. 103 (2006).
[248] *Id*. at 107.
[249] *Id*.
[250] *Id*.
[251] *Id*.
[252] *Id*. at 106.
[253] *Id*.
[254] *Id*. at 111. *Randolph* elaborated on "widely shared social expectations" as "influenced by the law of property" and stemming from social "understandings that are recognized and permitted by society." *Id.*
[255] *Id*.
[256] *Id*. at 111-12.
[257] *Id*. at 111.
[258] *Id*. While *Randolph* conceded that "some group living together might make an exceptional arrangement that no one could admit a guest without the agreement of all," such a prospect of so "eccentric a scheme" was too remote to consider. *Id*. at 111-12. *Randolph* thus reasoned that *Matlock* "relied on what was usual and placed no burden on the police to eliminate the possibility of atypical arrangements." *Id.*

landlord or hotel manager who would not possess the authority to admit guests in the absence of the current occupant's consent.[259] *Randolph* even offered the instance where common authority to consent existed but was limited:

> [A] child of eight might well be considered to have the power to consent to the police crossing the threshold into that part of the house where any caller, such as a pollster or salesman, might well be admitted … but no one would reasonably expect such a child to be in a position to authorize anyone to rummage through his parents' bedroom.[260]

The Court in *Randolph* then applied its widely-shared social expectations test, concluding, "a caller standing at the door of shared premises would have no confidence that one occupant's invitation was a sufficiently good reason to enter when a fellow tenant stood there saying, 'stay out.'"[261] *Randolph* therefore ruled, "[s]ince the co-tenant wishing to open the door to a third party has no recognized authority in law or social practice to prevail over a present and objecting co-tenant, his disputed invitation, without more, gives a police officer no better claim to reasonableness in entering than the officer would have in the absence of any consent at all."[262]

The Court applied *Randolph's* "widely shared social expectations" rule in its most recent third party consent case, *Fernandez v. California*.[263] In *Fernandez*, an officer knocked on the door of an apartment "from which screams had been heard."[264] Roxanne Rojas, who answered the door, appeared red-faced and crying, with a "large bump on her nose," and blood on her shirt from a seemingly recent injury.[265] When the officer sought entry, Fernandez declared, "'You don't have any right to come in here. I know my rights.'"[266] Having probable cause to believe Fernandez assaulted Rojas, the officer arrested Fernandez, taking him to the police station.[267] About an hour later, a detective returned to the apartment, obtained consent from Rojas to enter and search, and recovered evidence linking Fernandez to a robbery.[268]

Fernandez confronted the very situation that *Randolph* considered—a conflict between two occupants about whether police might enter—but with the crucial difference that the police had removed the objecting occupant from the premises.[269] This factual difference did not require a new test, for the Court still inquired about the "customary social usage" in deciding the case.[270] The Court in *Fernandez* acknowledged that "a caller" would feel uncomfortable accepting an invitation from one occupant if the other commanded she "stay out."[271] The caller's hesitation would stem from an expectation of "at best an

[259] *Id*. at 112.
[260] *Id*.
[261] *Id*. at 113.
[262] *Id*. at 114.
[263] Fernandez v. California, 571 U.S. 292, 303 (2014).
[264] *Id*. at 295.
[265] *Id*.
[266] *Id*. at 296.
[267] *Id*.
[268] *Id*.
[269] *Id*. at 294.
[270] *Id*. at 303.
[271] *Id*. at 303-04.

uncomfortable scene and at worst violence if he or she trie[d] to brush past the objector."[272] This same visitor's "calculus" would be "quite different, however, if the objecting tenant was not standing at the door."[273] As the Court in *Fernandez* surmised, "when the objector is not on the scene (and especially when it is known that the objector will not return during the course of the visit), the friend or visitor is much more likely to accept the invitation to enter."[274]

The Court, from *Matlock* to *Fernandez*, has thus constructed two rules for third party consent cases: (1) assumption of risk[275] and (2) "widely shared social expectations."[276] These tests led the Court to consider typical reactions people might have in all sorts of relationships, whether as co-tenants,[277] estranged husband and wife,[278] landlord and tenant,[279] hotelier and guest,[280] or domestic violence sufferer and abuser.[281] Similarly, third party consent could offer guidance if law enforcement seeks consent from employers to access passive monitoring data. Since employees will choose to allow "joint access" to their employers to information from wearables, phone applications, and beacons, *Matlock* indicates that workers assumed a risk that their bosses might share this information with others, including police.[282] *Randolph's* "widely shared social expectations" thus requires the Court to consider the particulars of the corporate culture in which an employee found herself.[283]

Correctly applying *Randolph*'s social expectations principle to the employment context may require considering the context of *Fernandez*, which involved social expectations stemming from power imbalances between the parties involved in a violent domestic relationship. Although, hopefully not in a situation as nightmarishly dire as that facing a domestic violence victim, employees often face a power imbalance that can severely harm their bargaining position with their employer. Such power imbalances could explain, for instance, a UPS driver's acceptance of surveillance or an Amazon worker's acquiescence in restrictions on bathroom breaks. Such power imbalances raise concerns about voluntariness. While Roxanne Rojas did not countermand Fernandez's denial of entry to police, she let police come in when her abuser was absent and in police custody.[284] Similarly, employees will likely choose to avoid offending superiors in their aim to put food on the table. Employees, all too aware of the power employers hold over their financial fates, might fail to communicate their true concerns. Justice Souter noted a similar complication in his concurrence in *Davis v. United States*.[285] He explained, "[s]ocial science confirms what common sense would suggest, that individuals who feel intimidated

[272] *Id*.
[273] *Id*. at 304.
[274] *Id*.
[275] *Matlock*, 425 U.S. at 171, n. 7.
[276] *Randolph*, 547 U.S. at 111. As previously noted, *Fernandez* couched the "widely shared social expectations" inquiry as one of "customary social usage." *Fernandez*, 571 U.S. at 303.
[277] *Randolph*, 547 U.S. at 111.
[278] *Id*. at 106.
[279] *Id*. at 112.
[280] *Id*.
[281] *Fernandez*, 571 U.S. at 295.
[282] *Matlock*, 415 U.S. at 171, n. 7, 172.
[283] *Randolph*, 547 U.S. at 111.
[284] *Fernandez*, 571 U.S. at 296.
[285] Davis v. United States, 512 U.S. 452, 470 n. 4 (1994) (Souter, J., concurring).

or powerless are more likely to speak in equivocal or nonstandard terms when no ambiguity or equivocation is meant."[286] Employees, in short, through silence or hesitation, might slip into situations where they are sharing information that they would rather keep to themselves.

The Court considered voluntariness in *Schneckloth v. Bustamonte*, a case where a patrol officer searched a car he had stopped for having a burned out headlight and license plate light.[287] When other police arrived, after the six occupants of the car exited the vehicle, one of the officers asked if he could search the car.[288] One occupant, Alcala, replied in the affirmative.[289] The officers then found three stolen checks wadded up under the left rear seat, leading to charges against Bustamonte for possessing a check with intent to defraud.[290]

To define voluntariness of consent to search under the Fourth Amendment, the Court in *Schnecknoth* relied on precedent defining voluntariness of confessions under the Fourteenth Amendment.[291] The Court realized that voluntariness could not "be taken literally to mean a 'knowing' choice'" because even confessions extracted by coercion and brutality involved knowing the "choice of alternatives."[292] Determining the presence of voluntariness, instead, involved an inquiry into whether the person's actions were "the product of an essentially free and unconstrained choice."[293] If the individual did exercise such a choice, her will was respected; if not, then her will was "overborne" and her "capacity for self-determination critically impaired."[294] The Court assessed voluntariness by looking at "the totality of all the surrounding circumstances—both the characteristics of the accused and the details of the interrogation."[295] Since this inquiry weighed all the facts, voluntariness did not turn on any "single controlling criterion."[296] Therefore, the fact that a person might not know of his or her right to refuse to answer questions or give consent was not, in itself, controlling.[297] *Schneckloth* was careful to note, however, that any compulsion, even if implied or subtle, could undermine voluntariness.[298]

Such "implied or subtle" coercion could infect an employer-employee relationship possessing a bargaining power disparity. *Schneckloth* considered, relevant to the "totality of the circumstances," the "possibly vulnerable subjective state of the person who consents."[299] The Court, when weighing consent to passive monitoring, might therefore consider the relative power inherent in the employee's position in the company, her level of education, age, and sophistication.[300] This might mean the Court could offer more Fourth

---

[286] *Id*.
[287] Schneckloth v. Bustamonte, 412 U.S. 218, 220 (1973).
[288] *Id*.
[289] *Id*.
[290] *Id*. at 219-20.
[291] *Id*. at 223-24.
[292] *Id*. at 224.
[293] *Id*. at 225.
[294] *Id*.
[295] *Id*. at 226.
[296] *Id*.
[297] *Id*. at 226-27, 234. Such knowledge was, however, a relevant factor among the totality of the circumstances. *Id*. at 227.
[298] *Id*. at 227, 229.
[299] *Id*. at 229.
[300] *Id*. at 226.

Amendment protection to junior employees and less to supervisors. Further, instead of assessing the "details of the interrogation" in the employment context, the Court could consider the behavior of the company and the work environment that it has formed.[301] Finally, the fact that a particular employee was not aware of his rights in the company's employee handbook would not undermine consent. *Schneckloth* ruled that ignorance of one's constitutional rights, an even greater liability than ignorance of worker rights, did not make consent involuntary.[302] Any "totality of the circumstances" test for employee consent, relying as it does on all the particular facts of each individual case, fails to ensure consistent protection for workers in the future from police invasion of passive monitoring data. Thus, employee privacy protections need a sounder footing.

One potential employee protection might be supplied by *Garrity v. New Jersey*, a case in which the Court considered the coercive effects of a threat to one's job.[303] In *Garrity*, police officers in New Jersey were convicted of "conspiracy to obstruct the administration of the traffic laws."[304] Before questioning the officers about fixing traffic tickets, the Attorney General warned each officer, "that he had the privilege to refuse to answer if the disclosure would tend to incriminate him." However, the Attorney General also warned each officer "that if he refused to answer he would be subject to removal from office."[305] Given this choice, the officers answered the questions, resulting in their convictions.[306] The Court then considered whether "the fear of being discharged" for failing to answer questions "made the statements products of coercion in violation of the Fourteenth Amendment."[307] The choice "between self-incrimination or job forfeiture" was "likely to exert such pressure upon an individual as to disable him from making a free and rational choice."[308] Since voluntariness could be destroyed by coercion that was "mental as well as physical," *Garrity* recognized that "[s]ubtle pressures may be as telling as coarse and vulgar ones."[309] Choosing between a job and exercising a right was the "antithesis" of a free choice, infecting the statements with coercion in violation of the Fourteenth Amendment.[310]

Similarly, when employees choose to accept passive monitoring, they might be facing a coercive choice between maintaining their Fourth Amendment right to privacy and their only practical option for "their means of livelihood."[311] While it is true that they are making a calculated choice based on their own interests, choosing the lesser of two evils "does not exclude [the possibility of] duress."[312] To apply *Matlock* in reasoning that employees have "assumed the risk" of exposure in such a situation would defy daily experience. Workers in such a bind face a terrible risk with either choice. It is questionable

[301] *Id*. at 226.
[302] *Id*. at 226-27.
[303] Garrity v. New Jersey, 385 U.S. 493, 494-95 (1967).
[304] *Id*.
[305] *Id*. at 494.
[306] *Id.* The Court described the officer's choice as "a choice between the rock and the whirlpool." *Id.* at 495-96.
[307] *Id*. at 496.
[308] *Id*. at 496-97.
[309] *Id*. at 496.
[310] *Id*. at 497, 499. *Garrity* declared, "The option to lose their means of livelihood or to pay the penalty of self-incrimination is the antithesis of free choice to speak out or to remain silent."
[311] *Id*. at 497.
[312] *Id*. at 498.

whether the Court would consider *Garrity*, a Fourteenth Amendment due process case, in any Fourth Amendment consent case.[313] Yet, in *Schneckloth*, the Court borrowed its analysis of voluntariness for Fourth Amendment consent from the confession cases analyzed under Fourteenth Amendment due process.[314] Still, there is no guarantee that the Court would apply *Garrity* to passive monitoring cases. Ultimately, employees sharing personal data might be placing their privacy in jeopardy.

IV. CONCLUSION

There is some hope that the Court will protect employees from police access to employers' passive monitoring data. *Carpenter* could identify such information as so detailed and encyclopedic as to create the kind of "comprehensive chronicle" against which it deemed the Fourth Amendment should stand.[315] The Court could also choose to view the "operational realities" of workplaces implementing passive monitoring as still requiring privacy for intimate details such as the functioning of an employee's heart or the activities occurring in her bedroom.[316] Finally, the Court could determine that employees, in allowing "mutual use" and providing "joint access" to their personal information, still do not assume the risk that employers would share such details with the government because such consent would be counter to the "widely shared social expectations" in workplaces.[317] Yet, each relevant test, whether reasonable expectation of privacy, a workplace's operational realities, or social expectations, is dependent on how a future Court will view the details in a particular case and provides little certainty for privacy protection. Further, with the interminable advance of technologies intruding into our privacy, and the public's acceptance of these technologies' conveniences despite their invasiveness, privacy from passive monitoring is in danger. Digital intrusions are daily draining the reasonableness of privacy expectations. Further, companies continue to erode privacy in the workplace. In this context, employees who allow monitoring could be seen as assuming a risk that companies will share information, no matter how intimate.

Perhaps, to grapple with the privacy invasions of the twenty-first century, we should look to musings from the first century. Plutarch, the Greek biographer living in the Roman Empire, declared, "Character is habit long continued."[318] The actions we take, no matter our motives, tend to affect ourselves and, for that matter, the world. A decision we make in an instant out of expediency could, if continually repeated over time or imitated by others, change our lives. Employees, perhaps bewildered by the impact of ever-advancing technology in replacing human labor, the lingering effects of the 2008 global recession, or international trade, might simply feel that they have no good options. If employees want to

---

[313] *Id*. at 499. *Garrity* inquired, "Our question is whether a State, contrary to the requirement of the Fourteenth Amendment, can use the threat of discharge to secure incriminatory evidence against an employee."

[314] *Schneckloth*, 412 U.S. at 223. *Schneckloth* declared, "The most extensive judicial exposition of the meaning of 'voluntariness' has been developed in those cases in which the Court has had to determine the 'voluntariness' of a defendant's confession for purposes of the Fourteenth Amendment."

[315] *Carpenter*, 138 S. Ct. at 2211.

[316] *O'Connor*, 480 U.S. at 717.

[317] *Matlock*, 415 U.S. at 171 n.7; *Randolph*, 547 U.S. at 111.

[318] Plutarch, *Moralia, The Education of Children* (Loeb Classical Library ed. 1927), http://penelope.uchicago.edu/Thayer/E/Roman/Texts/Plutarch/Moralia/De_liberis_educandis*.html.

meet the mortgage or qualify for health insurance, they could reasonably swallow their objections and do the work needed to keep their jobs. This choice, while understandable, has costs. If an employee accepts passive monitoring today to get a needed pay raise, she may squander her privacy in the eyes of the Court tomorrow.

With the Court's current rulings, it might be necessary to view Fourth Amendment privacy as a precious resource that can be squandered if not carefully conserved. One employee, succumbing to the pressure of the moment, might have little effect on privacy doctrine. The accumulated choices of all workers, in contrast, could undermine our Fourth Amendment right to privacy. Such a prospect might seem terribly unfair, for it is those with the least power who are called upon, with each individual choice, to protect privacy for all. The existentialist philosopher, Jean-Paul Sartre, would offer little sympathy, as he once declared, "man is condemned to be free: condemned, because he did not create himself, yet nonetheless free, because once cast into the world, he is responsible for everything he does."[319] However troubled and limited our lot, we always have a choice about which actions we take. We cannot escape the consequences of our choices. We have to make privacy a priority for we might not be able rely on the Court's current precedent to do so. If we submit to passive monitoring, putting all our faith in the Court, the resulting stress from doubt could betray our sleepless nights and pounding hearts to our ever-watchful employers.

[319] Jean-Paul Sartre, *Existentialism is a Humanism*, 29 (Yale University Press 2007).