Maryland Law Review

Volume 81 | Issue 3 Article 5

Contact Tracing Cell Phone Apps and Wearable Devices: The Fourth Amendment Issues Confronting Public Employers

Marc Chase McAllister

CONTACT TRACING CELL PHONE APPS AND WEARABLE DEVICES: THE FOURTH AMENDMENT ISSUES CONFRONTING PUBLIC EMPLOYERS

MARC CHASE MCALLISTER*

* Marc McAllister is an Assistant Professor at Coastal Carolina University and previously taught law school courses on the Fourth Amendment. His articles have appeared in the *Boston College Law Review*, *Florida Law Review*, *Washington and Lee Law Review*, and *Alabama Law Review*. The author would like to thank Connor Ontiveros for his research assistance on this Article.

INTRODUCTION

Under the Occupational Safety and Health Act, employers have an obligation to provide a work environment "free from recognized hazards that are causing or are likely to cause death or serious physical harm."[1] According to the Occupational Safety and Health Administration ("OSHA"), COVID-19 falls within the scope of this law, and requires employers to take affirmative steps to reduce COVID-19-related hazards in the workplace.[2] Contact tracing technologies, the focus of this Article, are one way for employers to meet this legal obligation.[3]

Before COVID-19 upended American businesses in 2020, employers were tracking employee movements through technologies like Global

1. 29 U.S.C. § 654 (2018); *see also* Carrie Hoffman & John L. Litchfield, *Employer Use of Contact Tracing Apps: The Good, the Bad, and the Regulatory*, FOLEY & LARDNER LLP (July 7, 2020), https://www.foley.com/en/insights/publications/2020/07/employer-use-of-contact-tracing-apps. The Occupational Safety and Health Act applies to "a person engaged in a business affecting commerce who has employees, but does not include the United States (not including the United States Postal Service) or any State or political subdivision of a State." 29 U.S.C. § 652(5) (2018). Similar state laws apply to public employers. *See, e.g.*, Washington v. Union Carbide Corp., 870 F.2d 957, 962–64 (4th Cir. 1989) (noting that West Virginia's Occupational Safety and Health Act applies to public employers, as stated in W. VA. CODE §§ 21-3A-2(d)); Griffin v. Mullinix, 947 P.2d 177, 179 (Okla. 1997) (stating that Oklahoma's Occupational Safety & Health Standards Act applies only to public employers).

2. *See* OCCUPATIONAL SAFETY & HEALTH ADMIN., U.S. DEP'T OF LAB., OSHA 3990-03, GUIDANCE ON PREPARING WORKPLACES FOR COVID-19, at 17 (2020); *see also* Hoffman & Litchfield, *supra* note 1.

3. *See generally* Hoffman & Litchfield, *supra* note 1. *See also* Konrad Putzier & Chip Cutter, *Welcome Back to the Office. Your Every Move Will Be Watched*, WALL ST. J. (May 5, 2020), https://www.wsj.com/articles/lockdown-reopen-office-coronavirus-privacy-11588689725 (describing apps developed for contact tracing purposes). Contact tracing apps are not the only means of protecting employees from the virus. *See* OCCUPATIONAL SAFETY & HEALTH ADMIN., *supra* note 2, at 8–16 (setting forth numerous infection prevention measures for employers, including the promotion of frequent hand washing, encouraging workers to stay home if they are sick, establishing flexible work sites and work hours, routine disinfecting of surfaces, and many others).

Positioning System ("GPS") and smartphone apps.[4] The COVID-19 pandemic has rapidly accelerated the development and use of employee surveillance technologies,[5] with "some employers planning to track movements and gather personal information like never before in Western democracies."[6] This increase in employee surveillance is significant given the present uncertainty regarding the COVID-19 pandemic's expected duration.[7] In addition, tracking and contact tracing technologies will likely continue to be used by employers after the pandemic and may become more

4. *See generally* Reid Blackman, *How to Monitor Your Employees–While Respecting Their Privacy*, HARV. BUS. REV. (May 28, 2020), https://hbr.org/2020/05/how-to-monitor-your-employees-while-respecting-their-privacy (reporting that "[e]ven before Covid-19 . . . employers were ramping up their efforts to monitor employee productivity"); Susan Bassford Wilson, *Tracking Employees in the Age of COVID-19*, CONSTANGY, BROOKS, SMITH & PROPHETE, LLP (July 1, 2020), https://www.jdsupra.com/legalnews/tracking-employees-in-the-age-of-covid-19854/ (noting that "[c]ompanies have long debated the merits of video surveillance in the workplace, tracking employee vehicles with GPS, or monitoring employee movements via a smartphone application"). Before COVID-19, employers used GPS tracking devices to track workers' locations. *See* Jeffrey M. Hirsch, *Future Work*, 2020 U. ILL. L. REV. 889, 928 (2020).

5. News articles outlining the recent increase in employee location tracking and contact tracing abound. *See, e.g.*, Peter Grant, *Office App Makers Cashing in on Pandemic Safety Needs*, WALL ST. J. (Mar. 9, 2021), https://www.wsj.com/articles/office-app-makers-cashing-in-on-pandemic-safety-needs-11615294802 (reporting that "[i]nvestors are pouring money into phone apps that enable companies to monitor employees' movements and ensure they are complying with social distancing . . . protocols"); Putzier & Cutter, *supra* note 3 (reporting that "[m]any Americans heading back to the factory and the office as the coronavirus pandemic eases will soon begin to notice that their every move is being watched or recorded"); Blackman, *supra* note 4 (reporting that "[t]he fear of productivity losses [caused by the pandemic], mingling with the horror of massively declining revenues, has encouraged many [business] leaders to ramp up their employee monitoring efforts"); Ryan Browne, *The Gadgets and Software that Could Help Us Return to the Office*, CNBC (Aug. 3, 2020, 6:23 AM), https://www.cnbc.com/2020/08/03/the-gadgets-and-software-that-could-help-us-return-to-the-office.html (reporting that, in response to COVID-19, "[t]ech firms big and small have been developing everything from wearable devices to thermal imaging cameras to help businesses equip their office spaces for the future"); PUB. CITIZEN, WORKPLACE PRIVACY AFTER COVID-19, at 4 (2020), https://www.citizen.org/wp-content/uploads/Workplace-Privacy-after-Covid-19-final.pdf (reporting that "[f]ifty new apps and technologies have been released since the pandemic began, not accounting for existing, unchanged technologies that now are being marketed as workplace surveillance tools to combat COVID-19"); Dan Schawbel, *How Covid-19 Has Accelerated the Use of Employee Monitoring*, LINKEDIN (Aug. 17, 2020), https://www.linkedin.com/pulse/how-covid-19-has-accelerated-use-employee-monitoring-dan-schawbel/ (noting that "[c]ompanies have invested more in technology during the pandemic" to improve efficiencies, and "[w]hile 30 percent of companies monitored their employees back in 2015, it's estimated that an entire 80 percent of companies are doing so today"); Wilson, *supra* note 4 (stating that although employers have monitored employees in the past, "some employers are taking another look at employee monitoring as a means to help ensure employee safety and hinder the spread of COVID-19").

6. Putzier & Cutter, *supra* note 3.

7. *See* Daniela Hernandez & Drew Hinshaw, *As Covid-19 Vaccines Raise Hope, Cold Reality Dawns that Illness Is Likely Here to Stay*, WALL ST. J. (Feb. 7, 2021), https://www.wsj.com/articles/as-vaccines-raise-hope-cold-reality-dawns-covid-19-is-likely-here-to-stay-11612693803 (reporting that the COVID-19 virus might last for several years, if not indefinitely, like the flu).

technologically sophisticated, making it imperative to examine the legality of such surveillance.[8]

Focusing on public employers, this Article examines how the most commonly used contact tracing technologies impact the Fourth Amendment rights of employees.[9] More specifically, this Article examines whether employer use of contact tracing technologies amounts to a Fourth Amendment search or seizure, whether the workplace exception to the warrant requirement would permit contact tracing programs, and which specific technologies are most likely to be upheld as reasonable under relevant Fourth Amendment precedents.[10]

Although this Article's conclusions and proposals are outlined with greater specificity below, briefly stated, this Article concludes that the least invasive tracing technologies are contact tracing cell phone apps and wearable contact tracing devices provided by employers, which generally rely on Bluetooth rather than GPS technology.[11] For those technologies, in particular, this Article concludes that the Fourth Amendment is likely not implicated because an employer's use of such technologies would not constitute a Fourth Amendment search or seizure of the employees

8. *See* Will Knight, *Tech Could Be Used to Track Employees–in the Name of Health*, WIRED (May 17, 2020, 7:00 AM), https://www.wired.com/story/tech-used-track-employees-name-health/ (reporting that Ryan Calo, a professor at the University of Washington, warns that new surveillance measures used by employers may persist long after the pandemic); Putzier & Cutter, *supra* note 3 (quoting New York University professor of clinical law, Jason M. Schultz, as stating that "[e]mployers don't really have any incentives to remove surveillance once they install it"); *id*. (describing a social-distancing app developed by real-estate company, RXR, which plans to use the technology after the pandemic to ensure the most efficient use of space and "the overall wellness of our customers"); Hirsch, *supra* note 4, at 928 (stating that "past advances like the time clock and aptitude tests pale in comparison to what is already occurring now, which in turn is a far cry from what is on the horizon").

9. This Article is limited to public employers in the United States and to the Fourth Amendment implications of contact tracing by those employers. This Article does not address other potential legal issues involving contact tracing apps, including, for example, issues that might arise under the Americans with Disabilities Act. *See* Stephen R. Brown et al., *May an Employer Require the Use of a Contact Tracing App?*, WESTLAW J. CORP. OFFICERS & DIRECTORS LIAB., June 2020, at 1 (2020); *see also* Mark Barnes et al., *Going Back to Work: Employer Use of "Apps" on Employee PDAs/Smart Phones for COVID-19 Contact Tracing*, ROPES & GRAY (May 1, 2020), https://www.ropesgray.com/en/newsroom/alerts/2020/05/Going-Back-to-Work-Employer-Use-of-Apps-on-Employee-PDAs-Smart-Phones-for-COVID-19-Contact-Tracing (discussing various laws that may impact employer-based contact tracing); U.S. Equal Emp. Opportunity Comm'n, *What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws*, https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws (Dec. 14, 2021); U.S. EQUAL EMP. OPPORTUNITY COMM'N, EEOC-NVTA-2009-3, PANDEMIC PREPAREDNESS IN THE WORKPLACE AND THE AMERICANS WITH DISABILITIES ACT, https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act#20 (2020).

10. *See infra* Part IV.

11. *See infra* Section I.B.2 and I.C.

themselves, their devices, or their data.[12] Nevertheless, there may be instances where the Fourth Amendment is implicated by these technologies. For example, if an employee is *compelled* by her employer to don a wearable tracking device, such as a wearable GPS-enabled necklace, this would likely constitute a Fourth Amendment search under the physical trespass test espoused in *United States v. Jones*.[13] In that event, a court would have to determine whether the search is reasonable under relevant Fourth Amendment precedents.[14]

Assuming a search or seizure would occur, this Article concludes that an employer's use of contact tracing cell phone apps and wearable contact tracing devices falls within the scope of the workplace exception to the warrant requirement set forth in *O'Connor v. Ortega*.[15] Under that exception, this Article further concludes that employer use of these contact tracing technologies would be reasonable under the Fourth Amendment.[16] This is because such devices advance the legitimate and substantial employer purpose of minimizing COVID-19 infections amongst employees. Additionally, the degree of intrusion upon employees is minimal since no employee cell phone data is accessed and detailed location information is not gathered like it is with GPS tracking, and the scope of surveillance is reasonable given that these technologies do not track anyone's location outside of work.[17]

Before turning to that analysis, Part I of this Article summarizes the technologies that enable employers to track employee movements, including those developed in response to COVID-19. Part II then outlines the Fourth Amendment rights of public employers. Next, Part III summarizes key judicial rulings on employer-initiated GPS tracking, a precursor to more modern contact tracing methods, and highlights lessons learned from Fourth Amendment litigation in this area. With those lessons in mind, Part IV identifies and analyzes a series of employment-related Fourth Amendment issues raised by more recent forms of contact tracing, with a particular focus on the most commonly used tracing technologies: contact tracing apps and wearable contact tracing devices. Finally, Part V provides proposals for contact tracing by public employers.

12. *See infra* Section IV.B.
13. 565 U.S. 400 (2012); *see infra* notes 299–304 and accompanying text.
14. *See infra* notes 118–122 and accompanying text.
15. 480 U.S. 709 (1987); *see also infra* Section IV.C.1.
16. *See infra* Section IV.C.2–3.
17. *See infra* Section IV.C.2–3.

I. EMPLOYEE LOCATION TRACKING DEVICES AND TECHNOLOGIES

Before analyzing the lawfulness of contact tracing, this Part outlines various technologies that enable employers to track or trace the movements of employees. Technologies summarized in this Part include GPS devices installed in employee vehicles, smartphone apps specifically designed to combat COVID-19, wearable location monitoring devices, video monitoring of employees, and a host of cutting-edge technologies that could be repurposed for contact tracing purposes, including radio-frequency identification ("RFID") chips implanted in employees.

A. GPS Tracking of Employee Vehicles

Perhaps the most established form of employee location tracking is through GPS tracking devices that track employee vehicles. This tracking method has been used to track employer-owned and personally-owned vehicles. Moreover, employers have implemented this surveillance method with and without employee knowledge and consent, both in employee misconduct investigations and outside the investigative context.[18]

Employers have generally tracked employees with GPS devices in one of two ways. The first method involves employers surreptitiously installing a GPS tracking device on an employee's vehicle, without the employee's knowledge or consent, to investigate an individual employee as part of a workplace misconduct investigation.[19] The second method involves employers installing GPS tracking devices in an entire fleet of employee vehicles, often with employee knowledge and consent, for some noninvestigatory business-related purpose, such as to improve efficiency or collect regulatory information.[20] These forms of GPS tracking, including how legal challenges to these methods might impact the employee tracing methods used to combat COVID-19, are examined in Part III.

18. *See generally* Marc Chase McAllister, *GPS and Cell Phone Tracking of Employees*, 70 FLA. L. REV. 1265, 1293–310 (2019).

19. *See, e.g.*, Cunningham v. N.Y. State Dep't of Lab. (*Cunningham II*), 997 N.E.2d 468 (N.Y. 2013) (involving an employer's surreptitious GPS tracking of its employee's private vehicle); Elgin v. St. Louis Coca-Cola Bottling Co., No. 4:05CV970-DJS, 2005 WL 3050633 (E.D. Mo. Nov. 14, 2005) (involving an employer's surreptitious GPS tracking of its employee's company-owned van to investigate potential employee theft).

20. *See, e.g.*, Carniol v. N.Y.C. Taxi & Limousine Comm'n, 975 N.Y.S.2d 842 (Sup. Ct. 2013) (challenging employer's use of GPS tracking data generated by its GPS devices installed in over 40,000 City of New York taxis), *aff'd*, 2 N.Y.S.3d 337 (App. Div. 2015).

B. Contact Tracing by Cell Phone

Approximately ninety-five percent of the U.S. population owns a cell phone, with most of those devices being smartphones.[21] Most cell phones sold since 2003 are GPS-enabled, making most phones trackable by GPS.[22] Most cell phones are also equipped with Bluetooth technology.[23] These technologies have given rise to a variety of contact-tracing apps that seek to determine whether a phone's user has been in close proximity to the COVID-19 virus.[24]

Contact tracing is a core disease-control measure that has been used for centuries.[25] Contact tracing requires a reliable process of identifying potentially exposed or infected individuals, informing them of their potential exposure, and helping them take appropriate action to protect their health and prevent further transmission.[26] According to the Centers for Disease Control and Prevention ("CDC"), emerging technologies can assist in contact tracing and may greatly help with scaling up these activities as needed.[27]

Until recently, contact tracing used old-fashioned methods, such as people conducting interviews of infected individuals to determine their recent interactions with others.[28] The State of Massachusetts recently announced

21. Divya Ramjee, Pollyanna Sanderson & Imran Malek, *Covid-19 and Digital Contact Tracing: Regulating the Future of Public Health Surveillance*, 2021 CARDOZO L. REV. DE NOVO 101, 121 (2021).

22. Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 493–94 (2012).

23. *See* Jaycon Systems, *Bluetooth Technology: What Has Changed over the Years*, MEDIUM (Sept. 28, 2017), https://medium.com/jaycon-systems/bluetooth-technology-what-has-changed-over-the-years-385da7ec7154; *see also* Molly Wood, *Bluetooth Smart Improvements Appear in More Devices*, N.Y. TIMES (Oct. 29, 2014), https://www.nytimes.com/2014/10/30/technology/personaltech/bluetooth-improvements-appear-in-more-devices.html (reporting that "Bluetooth and Wi-Fi are in almost everything these days, and Bluetooth, in particular, is cheap to include and increasingly reliable").

24. Browne, *supra* note 5.

25. *Case Investigation and Contact Tracing: Part of a Multipronged Approach to Fight the COVID-19 Pandemic*, CTRS. DISEASE CONTROL & PREVENTION (Dec. 14, 2020), https://www.cdc.gov/coronavirus/2019-ncov/downloads/php/principles-contact-tracing-booklet.pdf [hereinafter *Case Investigation and Contact Tracing*]; *see also* Lawrence O. Gostin & James G. Hodge, Jr., *Piercing the Veil of Secrecy in HIV/AIDS and Other Sexually Transmitted Diseases: Theories of Privacy and Disclosure in Partner Notification*, 5 DUKE J. GENDER L. & POL'Y 9, 16 (1998).

26. *See Case Investigation and Contact Tracing*, *supra* note 25; *see also* Derek Thompson, *The Technology that Could Free America from Quarantine*, ATLANTIC (Apr. 7, 2020), https://www.theatlantic.com/ideas/archive/2020/04/contact-tracing-could-free-america-from-its-quarantine-nightmare/609577/ ("In its most basic form, tracing—otherwise known as tracking, or contact tracing—means identifying all the recent interactions of sick individuals to determine whom they might have infected. Testing plus tracing can besiege the virus, starve it of new bodies, and return the world to its previral routine, or something like it.").

27. *Case Investigation and Contact Tracing*, *supra* note 25.

28. Gostin & Hodge, Jr., *supra* note 25, at 14; Thompson, *supra* note 26.

plans to hire 1,000 people to conduct these types of interviews.[29] While commendable, this approach to contact tracing is not ideal, as it is limited by faulty memories of recent contacts and by the vast amount of personnel and other resources required to contact trace in the midst of a global pandemic.[30] Moreover, the possibility of transmitting COVID-19 between strangers and asymptomatic carriers makes traditional contact tracing limited in its capacity to identify potential exposures.[31] To enable more widespread and more reliable contact tracing, governments and employers are turning to cell phone apps.[32]

1. Contact Tracing by Cell Phone GPS

Contact tracing through cell phone apps can take different forms, with some apps relying on GPS technology (associated with location data), and others relying on Bluetooth technology (associated with proximity data).[33] The most intrusive forms of contact tracing are GPS-based apps and tracing systems that rely on cell phone location data, which are in use by various countries around the world.[34] These GPS-based apps track the locations and

29. Martha Bebinger, *Why Charlie Baker Thinks 'Contact Tracing' Cases May Help Mass. Slow—Or Stop—COVID-19*, WBUR NEWS (Apr. 3, 2020), https://www.wbur.org/commonhealth/2020/04/03/contact-tracing-coronavirus-massachusetts-baker.

30. *See* Luca Ferretti et al., *Quantifying SARS-CoV-2 Transmission Suggests Epidemic Control with Digital Contact Tracing*, SCIENCE (May 8, 2020), https://www.science.org/doi/10.1126/science.abb6936 (stating that "[t]raditional manual contact-tracing procedures are not fast enough for [COVID-19]"); Thompson, *supra* note 26 (recognizing that "[p]eople have faulty memories about who or what they've touched, or where they've been," and that "person-to-person interviews might be too slow to arrest a national pandemic accelerating through a population").

31. *See* Ramjee et al., *supra* note 21, at 105.

32. Thompson, *supra* note 26; *see also* Isobel Asher Hamilton, *Compulsory Selfies and Contact-Tracing: Authorities Everywhere Are Using Smartphones to Track the Coronavirus, and It's Part of a Massive Increase in Global Surveillance*, BUS. INSIDER (Apr. 14, 2020), https://www.businessinsider.com/countries-tracking-citizens-phones-coronavirus-2020-3?utm_source=markets&utm_medium=ingest#/#the-us-is-reportedly-gathering-data-from-the-ads-industry-to-get-an-idea-of-where-people-are-congregating-1 (reporting that "[g]overnments across the world are availing every surveillance tool at their disposal to help stem the spread of the novel coronavirus," including "our smartphones").

33. *See* Ramjee et al., *supra* note 21, at 111.

34. *See* HENRY KENYON, LOCATION RECORDING CONTACT TRACING APPS MUST BE SCRAPPED, AMNESTY SAYS (June 19, 2020), 2020 WL 3401911 (describing mobile device contact tracing apps in Bahrain, Kuwait, and Norway that use a centralized data collection method that expose users' location and personal data to potential government surveillance); *see also* Alan Z. Rozenshtein, *Disease Surveillance and the Fourth Amendment*, LAWFARE (Apr. 7, 2020, 1:54 PM), https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment (arguing that "if the government were to track people's movement by directly surveilling cellphones . . . that might violate a person's reasonable expectation of privacy"); Hamilton, *supra* note 32.

movements of individual cell phones and communicate that information to a centralized source, such as the national government.[35]

Relying in part on cell phone location data, South Korea utilizes a program of mass surveillance that consists of tracking individuals' phones, credit card records, surveillance videos, and face-to-face interviews.[36] This information is then compiled into a publicly available map that allows citizens to check whether they have been in contact with any infected individuals.[37] The system also enables the South Korean government to send text messages warning people that they may have been in close proximity to an infected individual.[38] The location given can be extremely specific.[39] *The Washington Post* reported, for example, that a text, sent to over one million phones, stated that an infected person visited the "Magic Coin Karaoke in Jayang-dong at midnight on Feb. 20."[40] According to Yoon In-jin, a professor of sociology at Korea University in Seoul, his country has seen "many virus patients getting ridiculed and judged for places they visited."[41] And "[e]ven with names redacted, there are cases where enough information was made public to deduce the patient's identity."[42] As a result, one woman reported that she stopped going to a bar popular with gay women: "If I unknowingly contract the virus . . . that record will be released to the whole country."[43] The woman added, "[i]t's as daunting as being outed in front of the public."[44]

2. Cell Phone Contact Tracing Through Bluetooth

Bluetooth is arguably the least invasive of the cell phone contact tracing methods.[45] An app that relies on Bluetooth essentially permits users' phones to communicate with each other when in close proximity.[46] Australia's contact tracing app is one example. Australia's app, called COVIDSafe,

35. *See* KENYON, *supra* note 34; Ramjee et al., *supra* note 21, at 112.

36. Min Joo Kim & Simon Denyer, *A 'Travel Log' of the Times in South Korea: Mapping the Movements of Coronavirus Carriers*, WASH. POST (Mar. 13, 2020), https://www.washingtonpost.com/world/asia_pacific/coronavirus-south-korea-tracking-apps/2020/03/13/2bed568e-5fac-11ea-ac50-18701e14e06d_story.html.

37. Hamilton, *supra* note 32.

38. Hamilton, *supra* note 32; Kim & Denyer, *supra* note 36.

39. Hamilton, *supra* note 32.

40. Kim & Denyer, *supra* note 36.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

45. *See* Ramjee et al., *supra* note 21, at 113 (stating that "Bluetooth technology is associated with fewer privacy risks than GPS").

46. *See* Timothy Zick, *Clouds, Cameras, and Computers: The First Amendment and Networked Public Places*, 59 FLA. L. REV. 1, 20 n.92 (2007).

enables cell phones to conduct a "digital handshake" when they come within five feet of each other, then notifies users if they have come into contact for longer than fifteen minutes with an infected person.[47] The app does not collect location data, and an infected person must consent to having their data shared.[48]

In America, consulting giant PriceWaterhouseCoopers ("PwC") has developed a cell phone app that uses Bluetooth to track employee interactions.[49] The PwC tracing device requires workers to either download an app on their cell phone or add the code for the contact tracing app to an existing corporate app, enter their work e-mail address, and consent to the data policy.[50] Once installed, the PwC app runs in the background throughout the day and uses Bluetooth and Wi-Fi data to determine employees' proximity to one another and the amount of time employees spend interacting.[51] If an employee reports a COVID-19 infection, management then enters the person's email address into the tracing system to identify other employees the individual has come in contact with during a specified time frame.[52] The system ranks each contact's risk level—high, medium, or low—based on the individual's proximity to the person with the virus.[53] In this respect, one's "risk factor is a calculation of distance and time, not location."[54] According to PwC, the app does not track anyone's location or analyze data outside of work.[55] Rather, the app uses geofencing to limit tracing to corporate offices only.[56] As of May 2020, more than fifty PwC clients had expressed interest in the device, including some of America's biggest banks, manufacturers, and energy companies.[57]

47. Kim Lyons, *Australia's COVIDSafe Contact Tracing App Already Has More than a Million Downloads*, VERGE (Apr. 26, 2020, 6:39 PM), https://www.theverge.com/2020/4/26/21237598/australia-coronavirus-contact-tracing-privacy.

48. *Id.*

49. Browne, *supra* note 5; Kif Leswing, *Companies Could Require Employees to Install Coronavirus-Tracing Apps Like This One From PwC Before Coming Back to Work*, CNBC (May 6, 2020, 8:24 AM), https://www.cnbc.com/2020/05/06/pwc-is-building-coronavirus-contact-tracing-software-for-companies.html.

50. Putzier & Cutter, *supra* note 3; *see also* Veronica Combs, *New Coronavirus Contact Tracing Tool Could Help Offices Reopen by Tracking Employees*, TECHREPUBLIC (Apr. 30, 2020), https://www.techrepublic.com/article/pwc-repurposes-iot-platform-to-make-contact-tracking-faster-and-easier-for-employers/.

51. Putzier & Cutter, *supra* note 3; Combs, *supra* note 50; *see also* Leswing, *supra* note 49 (describing how the PwC app works).

52. Combs, *supra* note 50.

53. *Id.*

54. *Id.* (quoting Rob Mesirow, the principal for IoT services at PwC).

55. Putzier & Cutter, *supra* note 3.

56. Combs, *supra* note 50.

57. Putzier & Cutter, *supra* note 3.

Similar to the PwC app, Social Safety has developed an app for employees' mobile devices that uses Bluetooth technology to detect the distance between other devices running the app.[58] According to the company's website, employers can "require [their] employees to install the app on their personal mobile devices and have it active from an armband [holding their phone] while they attend work."[59] Once deployed, Social Safety signals employees through sounds, vibration, and light display when employees come closer than six feet apart.[60] As employees get closer together, the alerts become more urgent.[61] In addition, "the app keeps a secure, private record of accidental close contact between people" so that the employer may notify employees of potential exposure when an infection occurs.[62]

Beyond the employment context, Google and Apple recently partnered on COVID-19 contact tracing technology that users may download to their cell phones.[63] The State of California, among others, has employed the contact tracing technology through an app that relies on Bluetooth to send alerts to phones that have been in close proximity to someone who tests positive for COVID-19.[64] The app, called CA Notify, can be enabled by iPhone users in their device's settings, and can be downloaded to Android devices through the Google Play Store.[65] After the app is activated, the individual's phone automatically exchanges a private key with another phone that is within Bluetooth range.[66] The key does not contain location data or any personally identifying information, and the keys change every fifteen

58. *The Social Safety App: Keeping Your Employees Safe Through Social Distancing,* SOC. SAFETY, https://socialsafety.app (last visited Mar. 5, 2022).

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*

63. *Apple and Google Partner on COVID-19 Contact Tracing Technology*, GOOGLE (Apr. 10, 2020), https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/.

64. *Slow the Spread of COVID-19*, CA NOTIFY, https://canotify.ca.gov (last visited Oct. 13, 2021). According to the California government, CA Notify uses Bluetooth Low Energy technology to exchange random codes with the phones of others who have opted in without revealing any information about the users. If another CA Notify user that has been near an individual in the last two weeks tests positive for COVID-19, the potentially exposed person will then receive an anonymous notification that they have potentially been exposed. *Id.*

65. *Id.*

66. Mitchell Clark, *Apple and Google's COVID Contact Tracing Tech Is Finally Coming to Their Home State of California*, VERGE (Dec. 7, 2020, 5:50 PM), https://www.theverge.com/2020/12/7/22159842/apple-google-covid-contact-tracing-tech-california.

minutes.[67] When someone tests positive, they can send a notification to every other person using the app whose phone virtually bumped into theirs, letting them know that they should get tested and quarantine.[68] Such exposure notification does not include any information about who exposed whom or when and where it happened.[69]

C. Wearable Contact Tracing Devices

A variety of "wearable trackers" have also been used by employers in lieu of cell phone apps. One company, Estimote, has sold wireless tracking beacons to companies like Amazon, Apple, and Nike for contact tracing purposes.[70] According to the company's website, workers can wear small wireless devices—resembling a keycard, watch, or small garage door opener—that remind them to keep a safe distance from one another.[71] The wearables work by transmitting "encrypted short-range wireless signals," which other wearables pick up and vibrate if they are too close.[72] The wearables also "remember these direct contact interactions."[73] In the event an employee becomes ill, a company can examine its contact tracing dashboard and identify other individuals who may be at risk.[74]

Other companies have developed similar technologies—usually embedded in bracelets or wristbands—that notify workers if they are too close together, permitting contact tracing and virus exposure notifications through Bluetooth, rather than GPS. Examples of those technologies include

67. *Id.*; *see also Slow the Spread of COVID-19*, *supra* note 64. According to the State of California, the system never collects or shares any location data or personal information with Google, Apple, California Health and Human Services, or other users. *Id.*

68. Clark, *supra* note 66.

69. *Id.*

70. Will Knight, *Tech Could Be Used to Track Employees – in the Name of Health*, WIRED (May 17, 2020, 7:00 AM), https://www.wired.com/story/tech-used-track-employees-name-health/.

71. ESTIMOTE, https://estimote.com/wearable/ (last visited Mar. 4, 2022).

72. *Id.*

73. *Id.*

74. *Id.*

AiRISTA Flow[75] and TraceSafe.[76] Another similar technology is Safezone,[77] which has been used by professional sports leagues, including the NBA.[78] Like cell phone apps that rely on Bluetooth, the Safezone tracing device is designed to record only user interactions as a function of distance and duration of contact, rather than location.[79]

Another similar technology is Universal Contact Tracing, which operates with Bluetooth beacons embedded in wristbands or badges.[80] As people go through their day, interactions between individual badge numbers are recorded, noting time, location, and duration.[81] This data is accumulated anonymously, remaining unused unless a COVID-19 diagnosis is reported.[82]

Another company has developed a similar technology, called Proximity Trace or TraceTag, that facilitates contact tracing through a device affixed to an employee's hardhat.[83] Like similar wearable devices, the Proximity Trace

75. AIRISTA, https://www.airistaflow.com/industries/government/social-distancing-and-contact-tracing/ (last visited Mar. 4, 2022) (describing a wireless device worn by employees—worn as a wrist strap, pendant, or key fob—that detects proximity to other tags using Bluetooth and alerts users that come within six feet of each other, noting further that "[t]he system can integrate securely with government databases and third-party applications").

76. TRACESAFE, https://web.archive.org/web/20201230063926/https://www.tracesafe.io/ (last visited Dec. 30, 2020) (describing TraceSafe as "a full suite of real-time location management services and contact tracing solutions enabled through advanced low-power bluetooth beacons in a variety of form factors to suit"); *TraceSafe Selected as Official Contact Tracing Solution for TD Garden*, TRACESAFE (Dec. 8, 2020), https://global-uploads.webflow.com/5f0b2c52fd55612aa6935ad5/5fceec40f759a26a71a195c0_TraceSafe%20Selected%20as%20Official%20Contact%20Tracing%20for%20TD%20Garden.pdf (explaining that TraceSafe utilizes a patented contact tracing bracelet).

77. KINEXON, https://kinexon.com/safezone (last visited Mar. 3, 2022) (describing an "ultra-lightweight wearable [that] actively warns users if they are too close to another," and noting that "[t]he proximity and duration of each contact is recorded and can be quickly accessed to trace and evaluate chains of infection").

78. Baxter Holmes, *NBA to Require Players to Wear Sensors as Part of Contact Tracing*, ESPN (Dec. 31, 2020), https://www.espn.com/nba/story/_/id/30628788/nba-require-players-wear-sensors-part-contact-tracing (reporting that the NBA plans to require players and staff to wear Kinexon SafeZone contact sensor devices on the team plane, the team bus, during practices, and to and from the arena or their home practice facility).

79. *See Technology,* KINEXON, https://kinexon.com/technology/safetag/ (last visited Mar. 3, 2022) ("The KINEXON SafeTag does not record any movement, position or health data of the employees. Only the distance between two sensors is measured and the duration of the contact. This measurement is independent of the contact location and completely pseudonymized as well as randomized.").

80. *Animation: How Universal Contact Tracing Works*, MICROSHARE, https://www.microshare.io/2020/06/18/animation-how-universal-contact-tracing-works/ (last visited Mar. 4, 2022) (describing its Universal Contact Tracing technology that secures occupants of a facility without the use of smartphone apps).

81. Microshare, Inc., *Animation: How Universal Contact Tracing Works*, YOUTUBE (June 22, 2020), https://www.youtube.com/watch?v=h9gWX3CAf_M.

82. *Id.*

83. *In the Time of COVID-19–How Will You Maintain Safe Working Distances?*, TRIAX, https://www.triaxtec.com/social-distancing-contact-tracing/ (last visited Mar. 4, 2024).

device provides workers with visual and audible alarms when they get too close to one another, and more passively collects and records worker interactions for contact tracing purposes.[84]

D. Video Monitoring of Employees at Work

Numerous contact tracing technologies have been developed that rely on hardware installed around the workplace, including cameras and sensors.[85] Amazon, for example, utilizes "Distance Assistant," which provides live feedback to employees on social distancing through a camera, a fifty-inch monitor, and a computer.[86] As people walk past the camera, a monitor displays live video with visual overlays to show if associates are within six feet of one another.[87] Individuals remaining six feet apart are highlighted with green circles, while those who are closer together are highlighted with red circles.[88] Amazon recently open sourced this technology so that anyone can create their own Distance Assistant.[89]

In a more robust version of camera-based tracking, the Network of Intelligent Camera Ecosystem ("NICE") Alliance "provides an infrastructure for gathering and sorting massive amounts of raw video data . . . from multiple cameras that is time and space relevant."[90] "This process of sorting and organizing is performed in real time as the video is produced," thus enabling "real time processing of big video data."[91] Once compiled, video is indexed and becomes easily searchable by the user.[92]

Working with Microsoft, the NICE Alliance is developing a system that could allow any connected camera to become a smart camera capable of detecting a lack of social distancing, unmasked individuals, or even fevers.[93]

---

84. *Id.*

85. *See* PUB. CITIZEN, *supra* note 5, at 10–11 (listing in Table 3 various tracking technologies that rely on cameras, sensors, etc.).

86. Brad Porter, *Amazon Introduces 'Distance Assistant,'* AMAZON (June 23, 2020), https://www.aboutamazon.com/news/operations/amazon-introduces-distance-assistant.

87. *Id.*

88. *Id.*

89. *Id.*

90. *Overview Version 1.0.1*, NICE ALL. 5 (2019), https://www.nicealliance.org/wp-content/uploads/2020/02/nice-overview-v1.0.1.pdf.

91. *Id.*

92. *Id.* For information on how NICE manages privacy concerns, see *Priv. & Sec. Specification Version 1.0.1*, NICE ALL. (2019), https://www.nicealliance.org/wp-content/uploads/2020/02/nice-privacy-and-security-specification-v1.0.1.pdf.

93. Hillary K. Grigonis, *Post Lockdown, Smart Cameras Could Help Enforce Mask Use and Social Distancing*, DIGIT. TRENDS (May 18, 2020), https://www.digitaltrends.com/photography/nice-alliance-pandemic-security-cameras/. The NICE Alliance is a group of several camera manufacturers working together to create an operating system where cameras from multiple brands can talk to each other. *Id.* The NICE system is designed to

The cameras could send a text alert to business owners when a location is too crowded or social distancing rules are violated, or even trigger a warning in public spaces, such as a warning light.[94]

The NICE system works by looking for specific scenarios and only uploading data to the cloud that meets specified criteria.[95] If the camera detects more than two people at an entrance, for example, the data would then be sent to the cloud.[96] Besides leaving much of the information off the cloud entirely, the system uses encryption on any personal ID.[97] Facial detection looks only for the presence of a face mask.[98] Moreover, the system can use seen attributes—such as the color of a shirt or a hat—to identify a person's location without sharing or recording their identity.[99]

E. Other Forms of Location Tracking

Along with the more mainstream forms of contact tracing described above, other tracking technologies are being developed that have the potential to become far more invasive. For example, one company recently developed a work badge that not only tracks the movements of employees, but also captures the tone and length of workplace conversations.[100] The data produced by the badge can then be used to analyze things such as how much time workers talk to individuals of a particular sex, how much time they spend speaking versus listening, and how much they move around in a day.[101]

In a potentially more invasive form of surveillance, employees of a Wisconsin company, Three Square Market ("32M"), recently had radio-frequency identification ("RFID") chips implanted in their forearms.[102] The company's stated goal for this technology is to make routine employee tasks more efficient by, for example, allowing employees to use the installed RFID chip to make purchases in the break room, open doors, and log in to their computers.[103] 32M has emphasized that its RFID technology does not

work with existing cameras, requiring just a router instead of the replacement of every camera in the system. *Id.*

94. Grigonis, *supra* note 93.

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. Hirsch, *supra* note 4; *see also There Will Be Little Privacy in the Workplace of the Future*, ECONOMIST (Mar. 28, 2018), https://www.economist.com/special-report/2018/03/28/there-will-be-little-privacy-in-the-workplace-of-the-future.

101. Hirsch, *supra* note 4, at 928.

102. Joseph Jerome, *Embedded Chip on Your Shoulder? Some Privacy and Security Considerations*, INT'L ASS'N OF PRIV. PRO. (Aug. 1, 2017), https://iapp.org/news/a/embedded-chip-on-your-shoulder-some-privacy-and-security-considerations/.

103. *Id.*

involve GPS tracking; however, the technology is capable of location tracking, potentially enabling an employer to track individuals on a round-the-clock basis.[104]

In their efforts to combat COVID-19, some employers have also developed a broader set of "health surveillance" technologies that rely, in part, on facial recognition scans.[105] One example is Health Pass by CLEAR.[106] Users can download the CLEAR app on their smartphones and enroll in the service by verifying their identity using facial recognition.[107] To enter the workplace, users snap a selfie to authenticate their identity and take a health quiz on possible COVID-19 symptoms.[108] Users then approach a CLEAR pod for screening, where they use their face or a QR code generated by the app to share their health data and verified ID.[109] Based on the results, they would then either be admitted to or rejected from the workplace.[110]

A similar facial recognition technology that can be used by both businesses and employers is PopID, which uses a person's face as their form of identification.[111] Users of the PopID technology sign up with a selfie, which is then translated into a secure digital key and stored in the PopID cloud.[112] Users who have saved payment information can then choose to be recognized at any PopID-enabled business by standing in front of a camera.[113] From there, the PopID cloud matches the encrypted image to the user's digital key and permits payment with just the user's face.[114] In the

104. *Id.* Likewise, in Sweden, about 3,000 people recently had a microchip implanted in their bodies in exchange for making their lives easier. For instance, rather than have a physical keycard to unlock doors, they can wave their hand that contains the chip to perform the same task. Alexandra Ma, *Thousands of People in Sweden Are Embedding Microchips Under Their Skin to Replace ID Cards*, INSIDER (May 14, 2018, 8:09 AM), https://www.businessinsider.com/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5#:~:text=Thousands%20of%20Swedes%20are%20having,%2C%20Agence%20France%2DPresse%20reported.

105. Bryan Walsh, *Exclusive: Biometric ID Company CLEAR to Offer Coronavirus Screening for Businesses*, AXIOS (May 10, 2020), https://www.axios.com/coronavirus-health-screening-digital-id-48f5ee5b-05c4-4b5e-8fda-4d2f59b946b0.html.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id.*

111. *With PopID, Your Face is Your ID*, POPID, https://www.popid.com/#howitworks (last visited Mar. 4, 2022).

112. *Id.*

113. *Id.*

114. *Id.*

employment context, PopID can be used as a means of providing "[s]implified building access and temperature check at work."[115]

II. THE FOURTH AMENDMENT AS APPLIED TO PUBLIC EMPLOYERS

Because there is no single privacy law in America, employees may be protected from privacy invasions by various laws, including federal and state statutes, tort law, and constitutional requirements.[116] This Part summarizes the most common workplace privacy claims advanced by litigants to challenge instances of employee tracking by public employers.[117]

When an employee of a public employer believes their privacy rights were violated, they will usually sue their employer under 42 U.S.C. § 1983 and allege a violation of her constitutional right to be free from "unreasonable searches and seizures" under the Fourth Amendment to the United States Constitution.[118] Although the Fourth Amendment contains over fifty words, its core protection is to prohibit "unreasonable searches and seizures."[119]

115. *Id.* PopID has other applications beyond the employment context, such as device-free payments at drive-through restaurants, kiosk login and ordering at restaurants, and ticketless entry to event venues. *Id.*

116. *See* Mauricio Paez & Mike La Marca, *The Internet of Things: Emerging Legal Issues for Businesses*, 43 N. KY. L. REV. 29, 40 n.68 (2016). Privacy-related statutes typically apply to specific industries or particular types of data. *Id.*

117. Because this Article focuses on workplace privacy claims under the Fourth Amendment, it does not address other laws that might apply to employer-initiated contact tracing. *See supra* note 9 and accompanying text. This Article also does not address contact tracing by private employers, which, given the lack of state action, are typically not subject to Fourth Amendment constraints. *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 613–14 (1989) (stating that "[t]he [Fourth] Amendment [protects] . . . persons against certain arbitrary and invasive acts by officers of the [g]overnment or those acting at their direction" (citing Camara v. Mun. Ct. of San Francisco, 387 U.S. 523, 528 (1967))). For alleged privacy invasions, private employers may face liability through tort law, including the tort of intrusion upon seclusion, which is commonly used to sue private employers for privacy invasions arising out of workplace searches and seizures. *See* RESTATEMENT OF EMP. LAW § 7.06 (AM. L. INST. 2015) (discussing the tort of intrusion); *see, e.g.*, Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1033–34 (N.D. Cal. 2014) (discussing a tort of intrusion claim based on an employer's search of an employee's cell phone); Koeppel v. Speirs, 808 N.W.2d 177, 181 (Iowa 2011) (involving a tort of intrusion claim challenging an employer's installation of a hidden video camera in the employee restroom); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 636 (Tex. Ct. App. 1984) (involving a tort of intrusion claim challenging an employer's search of an employee's locker). As noted, however, the question of whether a private employer's contact tracing program would lead to liability in tort is beyond the scope of this Article.

118. U.S. CONST. amend. IV; West v. Atkins, 487 U.S. 42, 48 (1988) ("To state a claim under § 1983, a plaintiff must allege the violation of a right secured by the Constitution and laws of the United States, and must show that the alleged deprivation was committed by a person acting under color of state law." (citing Parratt v. Taylor, 451 U.S. 527, 535 (1981))); *see, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 714 (1987) (involving a Fourth Amendment claim based on an employer's search of a public employee's office).

119. U.S. CONST. amend. IV; *see also* Pennsylvania v. Mimms, 434 U.S. 106, 108–09 (1977) ("The touchstone of our analysis under the Fourth Amendment is always 'the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security.'"

Expounding on this core protection, courts have broken Fourth Amendment analysis into three steps. In the first step, courts consider whether a Fourth Amendment "search" or "seizure" has occurred.[120] If a "search" or "seizure" has occurred, then courts turn to the second step to consider whether that action was "unreasonable," that is, in violation of the Fourth Amendment.[121] If such a constitutional violation is established, courts move to the final step by considering the proper remedy, if any, for the Fourth Amendment violation.[122] Each of these steps to Fourth Amendment claims are outlined in more detail below, with an emphasis on how the Fourth Amendment restrains public employers.

A. Step One: Determining Whether a "Search" or "Seizure" Has Occurred

In the first step of Fourth Amendment analysis, courts consider whether a Fourth Amendment "search" or "seizure" has occurred. This is the critical threshold issue in Fourth Amendment analysis because without a search or seizure, no Fourth Amendment action has occurred, without which there can be no Fourth Amendment violation.[123]

1. Fourth Amendment Seizures

Fourth Amendment claims may involve seizures of persons or seizures of property. Under Fourth Amendment precedent, a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[124] A seizure would occur, for example,

(quoting Terry v. Ohio, 392 U.S. 1, 19 (1968))); Carniol v. N.Y.C. Taxi & Limousine Comm'n, 975 N.Y.S.2d 842, 848–49 (Sup. Ct. 2013) (applying a general reasonableness analysis to an instance of employer-initiated GPS tracking), *aff'd*, 2 N.Y.S.3d 337 (App. Div. 2015); *see also* Rozenshtein, *supra* note 34 (noting that in Fourth Amendment special needs cases, courts generally "balance[] the intrusiveness of the search against the expected government benefits of that search and also ask[] whether the government could achieve its objective using less intrusive means").

120. United States v. Hartwell, 436 F.3d 174, 177 (3d Cir. 2006).

121. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353–54 (1967) (after finding that a "search and seizure" had occurred, examining "[t]he question remaining for decision . . . [of] whether the search and seizure conducted in this case complied with constitutional standards"); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (finding that no "search" had occurred, and therefore "no warrant was required").

122. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

123. *See* United States v. Raines, 536 F.2d 796, 801 n.6 (8th Cir. 1976); *see also* Martin R. Gardner, *Rediscovering Trespass: Towards a Regulatory Approach to Defining Fourth Amendment Scope in a World of Advancing Technology*, 62 BUFF. L. REV. 1027, 1030 (2014) ("It has long been understood that the Fourth Amendment is inapplicable without a 'search or seizure,' no matter how unreasonable a governmental intrusion would appear to be." (footnote omitted)).

124. United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citing United States v. Place, 462 U.S. 696 (1983)).

when police take a person's property into police possession.[125] In the employment context, a seizure of data might occur when an employer downloads the contents of an employee's private cell phone onto the employer's work computer in order to search those contents.[126]

Employment-related challenges involving seizures of persons are less common but sometimes occur. As a general principle, a person is seized under the Fourth Amendment when there has been "a meaningful interference with his freedom of movement."[127]

2. Fourth Amendment Searches

Under Fourth Amendment law, the term "search" is a legal term of art distinct from its ordinary dictionary definition.[128] To determine whether a Fourth Amendment "search" has occurred, courts typically apply the "reasonable expectation of privacy" test derived from *Katz v. United States*.[129] Under the *Katz* test, a Fourth Amendment "search" occurs when the government violates a person's expectation of privacy that society recognizes as reasonable or legitimate.[130]

Under the *Katz* test, whether an expectation of privacy is reasonable depends on context, and may turn on a host of factors.[131] In the employment context, the most significant factors affecting whether an employee may reasonably expect privacy include: (1) who owns the property subject to intrusion, recognizing that employees may typically expect greater privacy in personally-owned devices as opposed to property owned by their

125. *Id.* at 120 n.18.

126. *See* Larios v. Lunardi, 445 F. Supp. 3d 778, 782 (E.D. Cal. 2020).

127. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 616 (1989). *See generally* United States v. Davis, 94 F.3d 1465, 1467–68 (10th Cir. 1996) (summarizing the types of Fourth Amendment seizures).

128. *See* Kyllo v. United States, 533 U.S. 27, 32 n.1 (2001) (contrasting the Fourth Amendment definition of "search" with the dictionary definition of "search").

129. 389 U.S. 347 (1967).

130. *See id.* at 361 (Harlan, J., concurring) ("[T]here 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.'"); *see also Kyllo*, 533 U.S. at 33 (discussing this framework); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (speaking in terms of a "legitimate expectation of privacy," or "one that society is prepared to accept as objectively reasonable").

131. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (recognizing that "the reasonableness of an expectation of privacy . . . is understood to differ according to context"). *Compare* Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (finding, based on the particular facts of the case, that employee had a reasonable expectation of privacy in the contents of his office computer), *with* United States v. Barrows, 481 F.3d 1246, 1248 (10th Cir. 2007) (finding employee had no reasonable expectation of privacy in the contents of a personal computer he used at work).

employers;[132] (2) whether an employee has been notified of, and consented to, the employer's conduct;[133] and (3) whether the area or item searched was widely accessible, or instead accessible only to the individual claiming an expectation of privacy.[134] Additional factors that commonly affect expectations of privacy under Fourth Amendment precedents include: (4) the location of the search;[135] (5) the intrusiveness of the investigative technique;[136] and (6) the manner of investigation.[137]

132. *See, e.g.*, United States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

133. *See, e.g.*, *Simons*, 206 F.3d at 398 (recognizing that "office practices, procedures, or regulations may reduce legitimate privacy expectations" of government employees in their offices); United States v. Sihler, 562 F.2d 349, 350–51 (5th Cir. 1977) (finding search of employee justified by consent where sign at entryway stated that all persons entering the workplace "are subject to routine searches of their person, property or packages" (emphasis omitted)); United States v. Esser, 284 F. App'x 757, 759 (11th Cir. 2008) (same as *Sihler*); *see also* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 655 (Cal. 1994) (recognizing that "the presence or absence of opportunities to consent voluntarily to activities impacting privacy interests obviously affects the expectations of the participant"); United States v. Yudong Zhu, 23 F. Supp. 3d 234, 240–41 (S.D.N.Y. 2014) (upholding computer search over Fourth Amendment challenge in part because employee gave written consent to inspection); United States v. Hamilton, 778 F. Supp. 2d 651, 654 (E.D. Va. 2011) (finding public school employee could not reasonably expect privacy in e-mails with his wife stored on his work computer because he knew contents of his computer were subject to inspection).

134. *See O'Connor*, 480 U.S. at 718 (recognizing that "some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable"). Regarding this factor, an employee could not reasonably expect privacy in most activities conducted in an open-air cubicle at work, such as a telephone conversation occurring within earshot of a fellow employee. *See id.* On the other hand, "if [an] employer equips the employee's office with a safe or file cabinet or other receptacle in which to keep his private papers, he can assume that the contents of the safe are private." Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (citing *O'Connor*, 480 U.S. at 718–19).

135. In the criminal investigation context, for example, the Supreme Court has ruled that dog sniffs do not constitute Fourth Amendment searches when the dog sniff occurs in the airport, *United States v. Place*, 462 U.S. 696, 707 (1983) (involving a dog sniff of a passenger's luggage), or on a public road, *Illinois v. Caballes*, 543 U.S. 405, 406, 410 (2005) (involving a dog sniff around an automobile lawfully stopped on the highway). On the other hand, the Supreme Court has ruled that use of a drug-sniffing dog on the front porch of a home is a Fourth Amendment search. Florida v. Jardines, 569 U.S. 1, 11–12 (2013).

136. Generally speaking, the closer one gets to a person's body, the more invasive the search or seizure becomes. A strip search, for example, requires a greater degree of suspicion than a search of a person's backpack or outer clothing. *See* Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 373–77 (2009) (upholding warrantless search of a teenage girl's backpack and outer clothing while striking down a search of her undergarments).

137. This factor is often significant when sophisticated technology is used in an investigation. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34–36 (2001) (striking down warrantless police use of a thermal imaging device to scan the outside of a suspect's home and recognizing that searches conducted via sophisticated technologies are fundamentally distinct from those that are not); United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (distinguishing GPS monitoring from "lawful conventional surveillance techniques").

Beyond these relatively common factors, any other relevant factor in the case at hand may impact whether an expectation of privacy is reasonable.[138] In addition, a person's status can fundamentally alter his or her expectations of privacy. Prisoners, public school students, and arrestees, for example, generally have reduced expectations of privacy as compared to ordinary adult citizens.[139] Along these lines, due to the nature of the employment relationship, employees generally have lesser expectations of privacy vis-à-vis their employers than they have in other contexts.[140]

As an alternative to the *Katz* test, courts sometimes apply the physical trespass test to determine whether a Fourth Amendment "search" has occurred.[141] Under this test, rather than examining whether it would be reasonable to expect privacy in the case, courts consider whether the government sought to obtain information by physically intruding on a constitutionally protected area, such as a "house" or "effect."[142] Such a trespass occurs when a government agent, without consent, encroaches an area or object protected by the Fourth Amendment, such as a vehicle or a home, in order to find something or obtain information.[143]

The physical trespass test, while important, has not been applied to employer-initiated investigations as often as the reasonable expectation of privacy test.[144] This is mostly due to the historical development of the two

138. *See* State v. Granville, 423 S.W.3d 399, 407–08 (Tex. Crim. App. 2014) (listing factors courts use in deciding whether a person has a reasonable expectation of privacy in the place or object searched); State v. Tentoni, 871 N.W.2d 285, 288 (Wis. Ct. App. 2015) (listing similar factors); Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 179 (1st Cir. 1997) (citing common factors as including whether the work area in question was given over to an employee's exclusive use, the extent to which others had access to the work space, the nature of the employment, and whether office regulations placed employees on notice of potential employer intrusions).

139. *See* Maryland v. King, 569 U.S. 435, 463 (2013) (stating that a person's "expectations of privacy and freedom from police scrutiny are [often] reduced" after an arrest); State v. Kisack, 236 So. 3d 1201, 1204 (La. 2017) (per curiam) (recognizing that "prisoners have a reduced expectation of privacy" under Fourth Amendment law); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 656–57 (1995) (recognizing that K-12 students have a reduced expectation of privacy); *see also* Bernard James, T.L.O. *and Cell Phones: Student Privacy and Smart Devices After* Riley v. California, 101 IOWA L. REV. 343, 350–51 (2015) (discussing K–12 cases).

140. *See* O'Connor v. Ortega, 480 U.S. 709, 723–25 (1987); RESTATEMENT OF EMP. LAW § 7.01 cmt. b (AM. L. INST. 2015) (recognizing that "employees have different expectations of privacy than they may have outside of the workplace").

141. *See* United States v. Cowan, 674 F.3d 947, 955 (8th Cir. 2012).

142. Florida v. Jardines, 569 U.S. 1, 5 (2013); *see also* U.S. CONST. amend. IV (establishing, in pertinent part, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures").

143. United States v. Jones, 565 U.S. 400, 410 (2012); *Jardines*, 569 U.S. at 11 ("That the officers learned what they learned only by physically intruding on Jardines' property to gather evidence is enough to establish that a search occurred."); *id.* at 7–10 (discussing the lack of consent by Jardines).

144. *See generally* Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 741 (2019) (recognizing that searches are currently "largely defined by the *Katz* test").

tests—the physical trespass doctrine dominated Fourth Amendment jurisprudence in the early 1900's, whereas the reasonable expectation of privacy test took center stage as a result of the Court's 1967 decision in *Katz*.[145] Due to *Katz*'s emphasis on expectations of privacy, the physical trespass test became less prominent in search analysis until it was revived by the United States Supreme Court in 2012.[146] Thereafter, courts began considering both tests in modern "search" cases.[147]

B. Step Two: Determining Whether the Search or Seizure is "Reasonable"

If a court determines that a Fourth Amendment search or seizure has occurred, the court then determines whether the search or seizure was reasonable.[148] Exactly what makes a search or seizure reasonable varies by context. In the criminal investigation context, warrants and probable cause are often required for a search or seizure to be reasonable.[149] Neither warrants nor probable cause are required, however, when a search or seizure is conducted for a non-law enforcement, or a "special needs" purpose, as in the case of searches conducted by public school officials,[150] building inspectors,[151] and public employers.[152] Because such government actors are usually not engaged in criminal investigations, where warrants and probable

145. *See Jones*, 565 U.S. at 406 (noting that "for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates"); Katz v. United States, 389 U.S. 347, 351 (1967) (declaring that "the Fourth Amendment protects people, not places").

146. *See Jones*, 565 U.S. at 405–06; United States v. Johnson, 871 F. Supp. 2d 539, 546 (W.D. La. 2012) ("*Jones* established, or perhaps reiterated, that there are two ways to analyze [whether a Fourth Amendment 'search' has occurred]: a traditional common-law property rights test and the *Katz*/reasonable-expectation-of-privacy test.").

147. *See Jones*, 565 U.S. at 404–07. In *Jones*, the Court held that a Fourth Amendment search occurred when police obtained location information by trespassorily attaching a GPS tracking device to a criminal suspect's vehicle. *Id.* at 404. The Court did not reach the question of whether a search would have occurred under the alternative reasonable expectation of privacy test. *Id.* at 406. *See generally* Kathryn E. Fifield, *Let This Jardines Grow: The Case for Curtilage Protection in Common Spaces*, 2017 WIS. L. REV. 147, 158–60 (2017) (discussing the historical development of the two search tests and concluding that the two tests "now exist side by side in Fourth Amendment jurisprudence").

148. *See supra* note 121 and accompanying text.

149. *See Katz*, 389 U.S. at 357 ("Over and again this Court has emphasized that . . . searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (footnote omitted)). Although warrants require a showing of probable cause, U.S. CONST. amend. IV, many warrant exceptions also require probable cause. *See* McAllister, *supra* note 18, at 1273 n.42.

150. *See* New Jersey v. T.L.O., 469 U.S. 325, 340–41 (1985).

151. *See* Camara v. Mun. Ct. of San Francisco, 387 U.S. 523, 528 (1967).

152. *See* O'Connor v. Ortega, 480 U.S. 709, 720–25 (1987) (rejecting the warrant and probable cause requirements in the employment context).

cause are more appropriate, their actions must instead be "reasonable[] under all the circumstances," a requirement that is less rigorous than probable cause.[153]

In the employment context, to be "reasonable[] under all the circumstances," a search or seizure must be both reasonable at its inception and reasonable in scope.[154] According to the United States Supreme Court's opinion in *O'Connor v. Ortega*, a search by an employer will be *reasonable at its inception* when the employer has "reasonable grounds for suspecting" either (a) that the search will turn up evidence that the employee is guilty of work-related misconduct (like a suspected company theft), or (b) that the search is necessary for a noninvestigatory, work-related purpose (like entering an office to retrieve a needed file).[155] Built into these standards is a requirement that the search be "work-related," or based on some legitimate employer interest.[156] In addition, as used here, the term "reasonable grounds for suspecting" is synonymous with the Fourth Amendment's reasonable suspicion standard,[157] one that is less demanding than probable cause.[158]

According to *O'Connor*, a search will be *reasonable in scope* when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of [either] the nature of the [suspected] [misconduct]" or the overall circumstances giving rise to the search.[159] Under this standard, the suspicion that justifies the search helps delineate its

153. *O'Connor*, 480 U.S. at 725–26; *see also id.* at 723–24 (recognizing that "public employers must be given wide latitude to enter employee offices for work-related, noninvestigatory reasons," and reaching a similar conclusion for searches conducted pursuant to an investigation of work-related employee misconduct).

154. *See id.* at 725–26.

155. *Id.*

156. *See, e.g.*, Ontario v. Quon, 560 U.S. 746, 761 (2011).

157. *O'Connor*, 480 U.S. at 724 ("The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest."). Although *O'Connor* sometimes used the phrase "reasonable grounds for suspecting," this phrase has been used by the Supreme Court in Fourth Amendment cases as a substitute for the "reasonable suspicion" standard. *See* United States v. Vinton, 594 F.3d 14, 25 (D.C. Cir. 2010) (recognizing that the Court's phrase "reasonable to believe" "probably is akin to the 'reasonable suspicion' standard"). Moreover, the *O'Connor* language itself has been interpreted by courts as requiring a showing of "reasonable suspicion." *See Cunningham II*, 997 N.E.2d 468, 473 (N.Y. 2013).

158. Comparing these two standards, the Supreme Court summarized "the required knowledge component of probable cause" as "rais[ing] a 'fair probability' or a 'substantial chance' of discovering evidence of criminal activity," and described "[t]he lesser standard" of reasonable suspicion as "a moderate chance of finding evidence of wrongdoing." Safford Unified Sch. Dist. No. 1 v. Redding, 557 U.S. 364, 371 (2009) (citation omitted).

159. *O'Connor*, 480 U.S. at 726 (third alteration in original) (quoting New Jersey v. T.L.O., 469 U.S. 325, 326 (1985)).

permissible scope.[160] For example, if an employer has sufficient reason to believe an employee has a red-colored file in her office that contains evidence of certain employee misconduct, the employer would be justified in entering that office and searching through any file cabinet or container large enough to hold that particular file.[161] Importantly, however, the right to search for the file extends only to those areas where it could reasonably be concealed.[162] Accordingly, in this example, it would not be reasonable to search inside a tiny pill bottle, nor would it be reasonable to search through a box of manila-colored files. Finally, once the red-colored file is found, the search should end so as to be no more intrusive than necessary.[163]

Beyond these basic requirements, *O'Connor* emphasized that judicial oversight of public employer searches would not be particularly rigorous and that public employers should be afforded "wide latitude" to perform such intrusions.[164] On the other hand, the Court suggested that the "workplace" exception to the warrant requirement would not apply beyond "the boundaries of the workplace context" itself, which the Court delineated as "those areas and items that are related to work and are generally within the employer's control."[165] As an example, the Court pointed to a hospital, where

160. *See, e.g.*, *Quon*, 560 U.S. at 761 (finding employer's review of text message transcripts reasonable because it was an efficient and expedient way to determine whether overages were the result of work-related messaging or personal use); *see also* Zimmerman v. Knight, 421 F. Supp. 3d 514, 522–23 (S.D. Ohio 2019) (discussing whether an employer's download of 2,731 pages of text messages, photographs, web browser history, and call history from Plaintiff's cell phone was reasonable in scope by examining whether the downloaded material was relevant to the employee misconduct inquiry).

161. *Cf.* WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, PRINCIPLES OF CRIMINAL PROCEDURE: INVESTIGATION 218 (Thomson West 2004) (discussing scope of consent principles, and stating that "when the object the police indicated they are looking for could be concealed therein, they may even search unlocked containers found in that place").

162. *See* JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE, VOLUME 1: INVESTIGATION 257 (5th ed. 2010) (discussing scope of search principles under the Fourth Amendment, and recognizing that "it would be improper for [the searching party] to open a container too small to hide the object of the search").

163. *See* RESTATEMENT OF EMP. LAW § 7.06 cmt. f (AM. L. INST. 2015) (recognizing, under the tort of intrusion, that "[i]f the scope [of search] extends beyond the purpose of the intrusion in furthering the employer's legitimate business interest, the intrusion is unjustified"); *see also, e.g.*, Mincey v. Arizona, 437 U.S. 385 (1978) (upholding an immediate warrantless search of a home for potential homicide victims by officers inside the home when a shooting occurred, but striking down a subsequent warrantless search of the entire premises by different officers occurring after the emergency ended); *Cunningham II*, 997 N.E.2d 468, 473 (N.Y. 2013) (finding an employer's thirty-day surreptitious GPS tracking of its employee's private vehicle unlawful because unreasonable in scope).

164. *See O'Connor*, 480 U.S. at 723–25. This is because, according to the Court, the employer's interest in efficient operation of the workplace is "substantial," whereas employees have limited expectations of privacy at work, which "are far less than those found at home or in some other contexts." *Id.* at 724–25.

165. *Id.* at 715.

the workplace would include "hallways, [the] cafeteria, offices, desks, and file cabinets," which "remain part of the workplace context even if the employee has placed personal items in them."[166] The Court cautioned, however, that "[n]ot everything that passes through the confines of the business address can be considered part of the workplace context."[167] The Court noted, for example, that the workplace exception "does not necessarily apply to a piece of closed personal luggage . . . that happens to be within the employer's business address," such as when an employee brings "closed luggage to the office prior to leaving on a trip" (presumably because such an item would not be one that is "related to work and . . . generally within the employer's control").[168]

In sum, *O'Connor* provides five important lessons for searches by government employers. First, *O'Connor* established that public employees may reasonably expect privacy in the workplace, depending on the workplace's unique circumstances.[169] Second, *O'Connor* created the workplace exception to the warrant requirement, under which Fourth Amendment claims of public employees will often depend on whether the employer's actions were reasonable at the inception and reasonable in scope, rather than whether probable cause exists or a warrant is obtained.[170] Third, for a search to be reasonable at its inception, the employer must have "reasonable suspicion"[171] to believe either that the search will turn up evidence of work-related misconduct, such as a suspected company theft, or "that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file" from an employee's office.[172] Fourth, to be reasonable in scope, the employer's search must not be "excessively intrusive" in light of the underlying justification for the search.[173] Finally, not every employer intrusion will fall within the scope of the workplace exception, as some items will not be within "the boundaries of the workplace context" if they are not sufficiently "related to work and . . . generally within the employer's control."[174]

166. *Id.* at 716.
167. *Id.*
168. *Id.* at 715–16.
169. *Id.* at 715–17.
170. *Id.* at 725–26.
171. *Id.* at 724; *see also supra* note 157.
172. *O'Connor*, 480 U.S. at 726.
173. *Id.* (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).
174. *Id.* at 715–16.

C. Step Three: Determining the Appropriate Remedy for a Fourth Amendment Violation

If the court finds that an unreasonable Fourth Amendment search or seizure has occurred, the court will then determine the appropriate remedy for the constitutional violation. In the criminal prosecution context, the usual remedy is exclusion of evidence obtained as a result of the Fourth Amendment violation.[175] Exclusion of evidence might also be appropriate in employee disciplinary proceedings.[176] But more commonly, in a 42 U.S.C. § 1983 civil suit based on an alleged Fourth Amendment violation by an employer, the usual remedy is money damages for the employee whose Fourth Amendment rights were violated.[177]

III. GPS TRACKING BY PUBLIC EMPLOYERS: LESSONS FROM RECENT CASES

Before COVID-19, employers used GPS tracking devices to investigate allegations of employee misconduct.[178] GPS tracking technology was also used for noninvestigatory work-related reasons, such as to collect regulatory information or to improve efficiency of operations.[179] Two recent cases from New York illustrate these distinct forms of GPS tracking. These cases are significant because they reach opposite results on the lawfulness of employee tracking and illustrate the types of factors courts will consider when deciding the constitutionality of contact tracing through cell phone apps and wearable devices.

In the first case, *Cunningham v. New York State Department of Labor*,[180] the Court of Appeals of New York examined an instance of GPS tracking conducted as part of an employee misconduct investigation by a New York state employer.[181] In 2008, to investigate its suspicion that employee Michael Cunningham was submitting false time sheets and taking unauthorized absences from work, the New York State Department of Labor ("the Department") attached a GPS device to Cunningham's car, without his

175. *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961).

176. *See, e.g.*, Cunningham v. N.Y. Dep't of Lab. (*Cunningham I*), 933 N.Y.S.2d 432, 435 (App. Div. 2011) (applying the exclusionary rule in an employee disciplinary proceeding), *rev'd*, 997 N.E.2d 468 (N.Y. 2013).

177. *See, e.g.*, K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984) (noting that a plaintiff-employee was awarded $108,000 in damages for an invasion of privacy by her employer).

178. *See infra* notes 180–195 and accompanying text (discussing *Cunningham I*).

179. *See infra* notes 196–214 and accompanying text (discussing *Carniol*).

180. *Cunningham I*, 933 N.Y.S.2d 432.

181. *Cunningham II*, 997 N.E.2d 468, 470–71, 475 (N.Y. 2013).

knowledge, while the car was parked in a lot near the Department's offices.[182] The device was then used to track the vehicle's movements for thirty days, including evenings, weekends, and several days when Cunningham was on vacation in another state.[183] GPS information showed that Cunningham's arrival and departure times from work were inconsistent with the number of hours he claimed on his time sheets.[184] The Department then brought thirteen charges of misconduct against Cunningham, eight of which were dependent on GPS evidence.[185] The Hearing Officer overseeing Cunningham's administrative proceeding sustained eleven of the thirteen charges and recommended termination of Cunningham's employment, which occurred shortly thereafter.[186]

Cunningham later sought to overturn his termination on the grounds that the GPS data used against him should have been suppressed as the fruit of a Fourth Amendment violation.[187] Applying the physical trespass test, the court first held that the GPS tracking of Cunningham's vehicle was a search under the Fourth Amendment.[188] The court then considered whether the warrantless search was reasonable under the *O'Connor* workplace exception.

Applying *O'Connor*, the court deemed the search justified at its inception because Cunningham's employer had "ample grounds to suspect him of submitting false time records."[189] The court deemed the search unreasonable in scope, however, as it involved "excessively intrusive," round-the-clock surveillance of Cunningham's vehicle,[190] which encompassed "much activity with which the State had no legitimate concern—i.e., it tracked [Cunningham] on all evenings, on all weekends and on vacation," capturing a great deal of purely private activity.[191]

Finally, the court addressed whether suppression of GPS data obtained during normal business hours was necessary since no evidence obtained from surveillance conducted outside of business hours was used against Cunningham.[192] Finding all GPS tracking data inadmissible, the court reasoned:

182. *Id.* at 470.

183. *Id.* at 470–71, 475.

184. *Id.* at 470–71.

185. *Id.*; *see also Cunningham I*, 933 N.Y.S.2d at 434.

186. *Cunningham I*, 933 N.Y.S.2d at 434.

187. Brief for Petitioner at 10, Cunningham v. N.Y. Dep't of Lab., 997 N.E.2d 468 (N.Y. 2013) (No. 2013-0123).

188. *Cunningham II*, 997 N.E.2d at 471.

189. *Id.* at 473.

190. *Id.* (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

191. *Id.*

192. *Id.*

> Ordinarily, when a search has exceeded its permissible scope, the suppression of items found during the permissible portion of the search is not required. But we hold that rule to be inapplicable to GPS searches like the present one, in light of the extraordinary capacity of a GPS device to permit "[c]onstant, relentless tracking of anything." Where an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable. That conclusion concededly requires suppression of [all] GPS evidence here . . . .[193]

Although *Cunningham* involved an employee misconduct investigation—a context distinct from the wholesale tracking of an entire segment of employees for noninvestigatory, business-related reasons—*Cunningham* is relevant for employers implementing more wholesale forms of employee tracking, such as contact tracing. As the quoted passage above shows, *Cunningham* reveals that when employers make no reasonable effort to avoid tracking an employee outside of business hours, the surveillance as a whole might be deemed unreasonable, leading to potential liability and money damages against the employer in a Fourth Amendment lawsuit.[194] Accordingly, if an employer conducts contact tracing through the more robust forms of contact tracing technologies described in Part I, such as GPS-based apps that capture detailed location data, the employer could face liability under the Fourth Amendment, suggesting that such contact tracing methods should be avoided.[195]

A second New York case, *Carniol v. New York City Taxi and Limousine Commission*,[196] is more directly analogous to contact tracing of an entire group of employees, as the case involved a Fourth Amendment challenge to an employer's tracking of an entire segment of employees for noninvestigatory reasons.[197] The events leading to this case began when the New York City Taxi and Limousine Commission ("TLC") mandated that all New York City medallion taxi cabs be equipped with GPS technology.[198] As originally developed, the TLC's intent was to gather data regarding pick-up and drop-off points, to assess trip time and distance, to eliminate the need for

193. *Id.* (alteration in original) (citations omitted) (quoting People v. Weaver, 12 N.Y.3d 433, 441 (2009)).

194. *See supra* Section II.C.

195. *See supra* Section I.B.1 (describing the South Korea app as an example). For these reasons, employers should avoid tracing technologies that would operate through RFID chips implanted in employees' bodies, as such technologies would clearly constitute a search under *Jones* and would likely be deemed excessively intrusive under *O'Connor*.

196. 975 N.Y.S.2d 842 (Sup. Ct. 2013), *aff'd*, 126 A.D.3d 409 (N.Y. App. Div. 2015).

197. *Id.* at 844–45.

198. *Id.* at 844.

drivers to complete handwritten trip sheets, and to assist in locating a passenger's lost property.[199]

With its administrative purposes in mind, the TLC did not plan to use the GPS system for investigatory purposes.[200] Yet, after receiving complaints that passengers were being overcharged, the TLC reviewed the data generated by the GPS system for essentially all of its 42,000 cab drivers, including Carniol.[201] After determining that Carniol had overcharged passengers ninety-one times, the TLC commenced an administrative proceeding against him, which resulted in the revocation of his TLC license.[202]

Carniol subsequently challenged the revocation, arguing that the TLC's use of GPS tracking violated his Fourth Amendment rights.[203] Under the first step of Fourth Amendment analysis, the Supreme Court for New York County ruled that Carniol could not legitimately expect privacy in the trip data gathered by GPS because the taxicab industry is heavily regulated and the GPS information was collected in furtherance of those regulations.[204] Assuming Carniol could expect privacy, however, the court went on to find that the TLC's GPS tracking program would have been reasonable in light of the competing interests at stake.[205]

According to the court, Carniol's "privacy interest" in the GPS-generated trip data was "minimal," and the "intrusion [was] also minimal," as "it [did] not involve a physical intrusion into Carniol's body or home" and did not collect data regarding his off-duty whereabouts.[206] On the other side of the scale, the government's interests in improving customer service and in regulating using "modern methods to promote passenger and driver safety" were "substantial."[207] The court further noted that the GPS monitoring was conducted with the knowledge and consent of the taxi driver and "was narrowly tailored to achieve a regulatory goal."[208] Accordingly, even if Carniol could legitimately expect privacy in the GPS data, the search would have been reasonable.[209]

For purposes of the instant analysis, five things are noteworthy about *Carniol*. First, because the GPS system at issue was installed with the

199. *Id.* at 844–45.
200. *See id.* at 845.
201. *Id.*
202. *Id.* at 845–46.
203. *Id.* at 846.
204. *Id.* at 848.
205. *Id.* at 848–49.
206. *Id.* at 849 (citation omitted).
207. *Id.*
208. *Id.*
209. *Id.*

knowledge and consent of the City's taxi drivers, the use of that system was not governed by *Jones*, leaving only the question of whether a Fourth Amendment search occurred under the *Katz* reasonable expectation of privacy test.[210] Second, taxi drivers subject to GPS monitoring could not reasonably expect privacy under *Katz*, at least in part because of their consent.[211] Third, that same consent contributed to the court's ultimate determination that the employer's wholesale GPS monitoring of its taxi drivers was reasonable.[212] Fourth, the legitimate government interests at issue—to regulate and improve the taxi industry through modern methods that better protect passenger and driver safety—tilted the scale of reasonableness in the employer's direction.[213] Finally, the fact that no data was collected regarding Carniol's off-duty whereabouts made the GPS surveillance relatively unintrusive as compared to *Cunningham*.[214]

When examining how *Cunningham* and *Carniol* might impact the more recent contact tracing technologies described in Part I, including contact tracing apps and wearable devices, it is important to consider the key differences between *Carniol* and *Cunningham* that generated opposite Fourth Amendment outcomes. Unlike *Cunningham*, the GPS tracking conducted in *Carniol* was done with employee consent, the employees in *Carniol* were not tracked while off-duty and away from work, and the legitimate employer interest of improving passenger and driver safety made the GPS tracking in *Carniol* even more reasonable. As the next Part shows, these same key ingredients—consent, limited scope, and legitimate employer interest—will help ensure that an employer's contact tracing program survives Fourth Amendment scrutiny.

IV. EMPLOYER CONTACT TRACING: THE FOURTH AMENDMENT ISSUES

There is currently no federal law that *directly prohibits* public employers from using contact tracing apps, wearables, and similar devices to track the movements of employees.[215] Certain state laws, however, could

210. *See id.*; *see also* United States v. Jones, 565 U.S. 400, 411 (2012) (recognizing that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis") (emphasis omitted).

211. *Carniol*, 975 N.Y.S.2d at 848 (emphasizing that the taxicab industry is heavily regulated, which reduces expectations of privacy, and that "the TTS system was installed with the knowledge of the taxicab owners and all taxicab drivers are required to follow TLC regulations which mandate the use of the TTS system").

212. *See id.*

213. *See id.* at 849.

214. *See id.*

215. Hoffman & Litchfield, *supra* note 1; Ramjee et al., *supra* note 21. In 2020, Congress proposed legislation on contact tracing, but thus far those bills have not been enacted into law. *See* Exposure Notification Privacy Act, S. 3861, 116th Cong. § 8 (2020) (introduced on June 1, 2020);

potentially impact employer use of such technologies.[216] More generally, public employers must ensure that such technologies comply with the Fourth Amendment, which requires consideration of the following issues:

- If employees consent to contact tracing by their employer, is their consent valid?
- If employee consent is presumed coerced and therefore invalid, what is the likelihood that a Fourth Amendment claim could materialize? Stated differently, would employer use of contact tracing technologies amount to a Fourth Amendment search or seizure?
- Assuming the Fourth Amendment applies, would the *O'Connor* workplace exception permit the employer's chosen contact tracing program?
- If the business justification for contact tracing is securing the health and safety of employees and others in the workplace, what is the permissible scope of such tracing?
- What does the permissible scope teach employers about which tracing technologies are most defensible under the Fourth Amendment?
- Would the current U.S. Supreme Court view widespread contact tracing by employers as a problematic version of suspicionless mass surveillance?

This Part examines these issues. For purposes of the instant analysis, this Part focuses on the more common types of contact tracing methods used by American employers today as outlined in Sections I.B.2 and I.C—i.e., contact tracing using cell phone Bluetooth data, and contact tracing accomplished through wearable devices that also primarily rely on Bluetooth. Because most employers today are not attempting to contact trace through GPS tracking devices or through a phone's internal GPS (described in Sections I.A and I.B.1), both of which raise great privacy concerns, this Part does not directly address the lawfulness of those surveillance methods.[217]

COVID-19 Consumer Data Protection Act of 2020, S. 3663, 116th Cong. (2020) (introduced on May 7, 2020); Public Health Emergency Privacy Act, S. 3749, 116th Cong. (2020) (introduced on May 14, 2020).

216. *See, e.g.*, CAL. PENAL CODE § 637.7(a), (d) (West 1998) (stating that "[n]o person or entity in this state shall use an electronic tracking device to determine the location or movement of a person," and defining "electronic tracking device" as "any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals"). Under the California statute, some of the wearable devices described in Section I.C might be considered an "electronic tracking device." *See also* 720 ILL. COMP. STAT. ANN. 5/21-2.5 (West 2014) (generally prohibiting persons in Illinois from using an electronic tracking device to determine the location or movement of a person, with an exception for consent, among others).

217. *See supra* notes 33–44 and accompanying text.

A. Validity of Consent

Recall that the first step in any Fourth Amendment claim is to determine whether a search or seizure has occurred, and the second step is to determine whether such action, assuming one occurred, was reasonable.[218] Under either of these steps, employee consent can play a critical role.[219] Accordingly, it makes sense to first examine the issue of consent.

If employees consent to contact tracing by their employer, the question becomes whether that consent is valid. Under Fourth Amendment precedents, for consent to be valid, it must be freely and voluntarily given, rather than coerced.[220] As articulated by the Supreme Court, "the question whether a consent to a search was in fact 'voluntary' or was the product of duress or coercion, express or implied, is a question of fact to be determined from the totality of all the circumstances."[221] In addition, to be valid, "consent [must be] a product of th[e] individual's free and unconstrained choice, rather than a mere acquiescence [to] a show of authority."[222] In the employment context, if an employee is required to submit to a search or seizure *as a condition of continued employment*, the employee's consent to that action might be considered coerced.[223]

One example of coerced consent in the employment context occurred in *Port Authority Police Benevolent Ass'n v. Port Authority of New York & New Jersey*.[224] In that case, a group of employees sued their employer, the Port Authority of New York and New Jersey ("Port Authority"), for allegedly violating their Fourth Amendment rights by searching their personal cell phones.[225] The events leading to that search began when a class of the Port

218. *See supra* Section II.A; *see also* United States v. Simons, 206 F.3d 392, 399–401 (4th Cir. 2000) (analyzing these two steps in the context of a search of an employee's office at work).

219. *See supra* note 208 and accompanying text (discussing the role of consent in *Carniol*); *see also supra* note 133 (providing case examples involving employee consent). Of course, along with the workplace exception to the warrant requirement, there is also a consent exception that could be invoked in employment cases.

220. Bumper v. North Carolina, 391 U.S. 543, 548 (1968).

221. Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973).

222. Anobile v. Pelligrino, 303 F.3d 107, 124 (2d Cir. 2002) (quoting United States v. Garcia, 56 F.3d 418, 422 (2d Cir. 1995)); *Bumper*, 391 U.S. at 549.

223. *See* Sabin v. Miller, 423 F. Supp. 2d 943, 949 (S.D. Iowa 2006) (finding genuine issues of material fact as to whether an employee's consent was the result of duress or coercion when the employee's supervisor told her that an investigator was going to talk with her, that she should "cooperate completely" with the investigator, and that, "[e]verything will be all right, as long as you do what they tell you to do" (alteration in original)). *See generally* Carr v. Mulhearn, 601 A.2d 946, 949 (R.I. 1992) (discussing the "more subtle forms of coercion in the workplace that sometimes blur the line between voluntariness and compulsion").

224. No. 15-CV-3526, 2017 WL 4403310 (S.D.N.Y. Sept. 29, 2017).

225. Plaintiffs also sued certain individuals involved in the cell phone searches, but the district court dismissed those claims on the basis of qualified immunity. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *1.

Authority Police Department ("PAPD") graduated from police academy training as Probationary Police Officers ("PPOs"), making their employment easily terminable.[226] The following day, many of these PPOs attended a post-graduation party at the Texas Arizona Bar & Grill, which became rowdy and disruptive.[227]

The next morning, Lieutenant Timothy McGovern opened a police misconduct investigation ("PIU") into those events with the goal of interviewing all PPOs who attended the party.[228] Before conducting interviews, McGovern warned PPOs that they "were required to cooperate in an investigation" and "could face termination" if they did not.[229] On the first day of PPO interviews, McGovern learned that PPOs who attended the party used a cell phone application called GroupMe to communicate with one another about the party.[230] For PPOs that participated in these GroupMe chats, McGovern instructed investigators to request to view those messages.[231] Before each interview, PPOs were again informed they had to "cooperate in this investigation,"[232] and were not informed they had the right to refuse the cell phone search.[233] As a result, many of the PPOs understood that they had no choice but to consent to the search and believed they would be fired if they did not.[234]

After investigators reviewed the contents of thirty-six employees' personal cell phones,[235] PPOs sued their employer and various individuals involved in the search alleging their phones had been unreasonably searched and seized under the Fourth Amendment.[236] Defendants first sought to justify their warrantless cell phone searches under the *O'Connor v. Ortega* workplace exception, which permits certain warrantless searches by employers that are reasonable at the outset and in scope.[237] District Court

226. *Id.* at *2 (stating that "because the PPOs were probationary employees, all of them could have . . . been fired for any non-arbitrary and non-discriminatory reason").

227. *Id.* at *1. At that party, PPOs reportedly damaged property, stole beer, touched other patrons inappropriately, and fought with a bouncer, who described the evening as "the 'worst night' he had 'ever worked.'" *Id.*

228. *Id.* at *1–2.

229. *Id.* at *2.

230. *Id.*

231. *Id.*

232. *Id.* at *3. "Interview transcripts reveal that during [at least] thirty-three of those interviews, PPOs were given the opportunity to speak with their union representative before acceding to the search." *Id.* at *2.

233. *Id.* at *3.

234. *See id.* (summarizing testimony of various PPOs on this point).

235. *Id.* at *2. The Port Authority did not own any of the phones, did not pay for them, and did not pay for the cellular service. *Id.* at *3.

236. *Id.*

237. 480 U.S. 709, 725–26 (1987).

Judge Kimba Wood rejected this argument, however, because the PPOs' "purely personal" cell phones were not within the "workplace context" as articulated in *O'Connor*.[238] Rather, like employees' homes, the PPOs' personal cell phones were not "related to work and . . . [not] generally within the employer's control."[239] Moreover, like the closed "handbag or briefcase" mentioned in *O'Connor*, the PPOs did not relinquish their legitimate expectation of privacy in the *contents* of their personally-owned cell phones.[240] Accordingly, the *O'Connor* exception did not allow their warrantless inspection.[241]

Judge Wood then rejected the defendants' second defense based on the PPOs purported consent.[242] As Judge Wood noted, to be valid, consent must "not be coerced, by explicit or implicit means, by implied threat or covert force."[243] And in the employment context, "[c]oercion may be found where one is given a choice between one's employment and one's constitutional rights."[244] Applying these principles, Judge Wood concluded that a reasonable jury could find that the PPOs' acquiescence was coerced.[245] Indeed, PPOs were told they could be fired if they did not cooperate with the investigation, causing them to believe that they must consent to the search to retain their jobs.[246] With no applicable warrant exception, Judge Wood thus concluded that "a warrant was required before initiating the searches."[247]

Under cases like *Port Authority*, if an employee is forced to choose between losing their job and accepting a condition of continued employment, such as submitting to a cell phone search, the employee's consent might be deemed coerced.[248] If an employee is faced with a similar ultimatum of either participating in an employer's contact tracing program or being terminated, it is possible that an employee's consent to such surveillance might likewise be deemed coerced, leaving the *O'Connor* workplace exception as the only potential justification for such surveillance, an issue discussed below in Section V.C.

238. *Port Auth. Police Benevolent Ass'n*, 2017 WL 4403310, at *5 (citations omitted).
239. *Id.* at *4 (quoting *O'Connor*, 480 U.S. at 715).
240. *See id.* at *4–5 (quoting *O'Connor*, 480 U.S. at 716).
241. *Id.*
242. *Id.* at *6.
243. *Id.* at *5 (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 228 (1973)).
244. *Id.* (quoting Anobile v. Pelligrino, 303 F.3d 107, 124 (2d Cir. 2002)).
245. *Id.* at *6.
246. *Id.*
247. *Id.*
248. *See id.* at *5; *see also* Sabin v. Miller, 423 F. Supp. 2d 943, 949 (S.D. Iowa 2006) (recognizing that "[t]he state may not coerce its employees 'into relinquishing a constitutional guarantee under threat of losing their employment'" (quoting Lesher v. Reed, 12 F.3d 148, 150 (8th Cir. 1994))).

Before turning to that analysis, it is important to recognize that the more employee-friendly view of consent as espoused in *Port Authority* might not carry the day. Indeed, recent Supreme Court precedent reveals that in some instances when an employer has imposed a term of employment upon its workers as a condition of continued employment, the workers' consent to that term of employment is not necessarily coerced. Simply put, because the workers could reject the term of employment and look for work elsewhere, their acceptance of that term constitutes adequate "consent."[249]

This more employer-friendly view of consent finds support in a recent Supreme Court opinion, *Lamps Plus, Inc. v. Varela*.[250] In that case, an employee of Lamps Plus, Inc., Frank Varela, brought a putative class action lawsuit against his employer after a hacker obtained the tax information of hundreds of employees and filed a fraudulent tax return in Varela's name.[251] Like most Lamps Plus employees, Varela had signed an arbitration agreement when he started work at the company, one that was ambiguous with regards to whether class-wide arbitration was permissible.[252] Nevertheless, Varela brought claims on behalf of a putative class of employees whose tax information had been compromised by suing Lamps Plus in federal court.[253] Lamps Plus then moved to compel arbitration on an individual rather than class-wide basis, and to dismiss the lawsuit.[254]

Finding that Varela must arbitrate his claims individually, the Supreme Court declared that the Federal Arbitration Act ("FAA") generally envisions individualized arbitration (as a default rule), rather than class arbitration.[255] The Court emphasized, however, that "[a]rbitration is strictly a matter of consent," such that courts must enforce whatever terms of arbitration the parties agree upon.[256] Because it was unclear whether the parties truly intended to permit class arbitration, which lacks the benefits of the default position of individual arbitration, the Court was unable to conclude that the parties actually agreed to arbitrate their disputes on a class-wide basis.[257]

Most importantly, the *Lamps Plus* Court acknowledged that the employer drafted the arbitration agreement and imposed the agreement on its

249. Samuel R. Bagenstos, *Consent, Coercion, and Employment Law*, 55 HARV. CIV. RTS.-CIV. LIBERTIES L. REV. 409, 418 (2020).

250. 139 S. Ct. 1407 (2019).

251. *Id.* at 1412.

252. *See id.* at 1413.

253. *Id.*

254. *Id.*

255. *Id.* at 1415. *See also id*. at 1418–19.

256. *Id.* at 1415 (alteration in original) (quoting Granite Rock Co. v. Teamsters, 561 U.S. 287, 299 (2010)).

257. *Id.* at 1415–16.

workers as a condition of continued employment.[258] Nevertheless, the Court concluded that both parties had freely entered into the agreement, which had to be upheld as written because of their mutual consent.[259] Simply put, even though the employees had no real say in the disputed terms, and even though the terms were clearly unfavorable to the employees, the Court viewed those terms to reflect the intent of both parties.[260]

For the instant analysis, *Lamps Plus* reveals that in some instances the Court will find that employees have validly consented to a term of employment imposed by their employer simply by choosing to remain employed under that term of employment.[261] After all, the employees in *Lamps Plus* willingly accepted their employer's arbitration provision by signing the provision and remaining employed, rather than seeking employment elsewhere.[262] If this principle were applied to employer-imposed contact tracing methods, then the same type of "consent" might override any Fourth Amendment challenge to contact tracing at work. Indeed, if an employee has consented to a search or seizure, the employee cannot typically expect privacy in that instance and the employer's action would generally not be unreasonable, thereby defeating any Fourth Amendment claim against that employer.[263]

258. *Id.* *See also id.* at 1430 (Kagan, J., dissenting) (acknowledging, along with Justices Ginsburg, Breyer, and Sotomayor, that Lamps Plus drafted the arbitration agreement at issue and had the opportunity to insert language expressly barring class arbitration if that was its intent).

259. *See id.* at 1415–17 (majority opinion) (finding that ambiguity in an arbitration provision does not provide a sufficient basis for concluding that the parties to the agreement agreed to undermine the central benefits of arbitration itself, including arbitration on an individual, rather than a class-wide, basis).

260. *See id.* at 1416 (emphasizing the importance of "giv[ing] effect to the intent of the parties" (quoting Stolt-Nielsen S.A. v. AnimalFeeds Int'l Corp., 559 U.S. 662, 684 (2010))). *See id.* at 1421–22 (Ginsburg, J., dissenting) (finding "irony" in the majority's reliance on mutual consent in upholding a term of employment that is clearly unfavorable to the employee even though the employee had no real power to bargain for different terms).

261. Another recent Supreme Court case that arguably supports this view of consent is *Epic Systems Corp. v. Lewis*, 138 S. Ct. 1612 (2018). In *Epic Systems*, the parties had entered into a contract providing for individualized arbitration proceedings to resolve any employment disputes between them. *Id.* at 1619–20. Each employee nevertheless sought to litigate their claims through class or collective actions in federal court. *Id.* at 1620. The employees argued that their agreements' requirement of individualized proceedings should be set aside as violative of the National Labor Relations Act ("NLRA"). *Id.* at 1622. Although the employers in *Epic Systems* had required their employees to sign the arbitration agreements as a condition of continued employment, *id.* at 1633 (Ginsburg, J., dissenting), the Court refused to strike down those agreements, in part due to the employees' consent. *See id.* at 1619 (majority opinion).

262. *See* Bagenstos, *supra* note 249, at 419.

263. *See supra* note 133 (containing case examples involving consent).

B. Step One: Fourth Amendment Threshold Issues

Although it is possible that employee consent to an employer's contact tracing program might be deemed coerced under precedents like *Port Authority*, this does not end the Fourth Amendment inquiry. Rather, one must still determine whether a Fourth Amendment "search" or "seizure" has occurred, including (1) whether the employee could otherwise reasonably expect privacy in the case at hand (the primary search test);[264] (2) whether the employer has sought to obtain information by physically intruding on a person, house, paper, or effect (the alternative search test);[265] (3) whether contact tracing programs amount to a seizure of the employee (under the law that governs seizures of persons);[266] and (4) whether there has been a meaningful interference with the employee's possessory interest in a device used to facilitate contact tracing, such as a personal cell phone, or in the underlying contact tracing data (the relevant seizure test for effects).[267] If any of those threshold tests are met, the Fourth Amendment is at play, at which point one must still determine whether the underlying search or seizure was reasonable. This Section examines these threshold issues.

1. Reasonable Expectation of Privacy Search Test

Regarding whether a "search" occurs when an employer utilizes a system of contact tracing through cell phone apps or other wearable devices, the question becomes whether employees may legitimately expect privacy in their movements and interactions with one another while at work. Based on video surveillance cases, the answer to that question is likely no.

Although video surveillance by employers takes many forms, the most analogous form of surveillance to the contact tracing technologies at issue is video surveillance in open office spaces, such as break rooms and common areas, where concerns of close or extended employee interactions would be heightened.[268] When video surveillance has been conducted in open office spaces, courts have generally permitted the surveillance based on the fact that it would be unreasonable for employees to assume that anything occurring in these areas would be private.[269] This is especially true when the cameras are

264. *See supra* note 130 and accompanying text.

265. *See supra* notes 143–144 and accompanying text.

266. *See supra* note 127 and accompanying text.

267. *See supra* notes 124–126 and accompanying text.

268. *Compare* Acosta v. Scott Lab., LLC, 377 F. Supp. 2d 647 (N.D. Ill. 2005) (involving video surveillance in open spaces), *with* Koeppel v. Speirs, 808 N.W.2d 177 (Iowa 2011) (involving a hidden video camera the employer placed in the female employees' restroom).

269. *See, e.g.*, *Acosta*, 377 F. Supp. 2d at 650 (recognizing that "[p]ersons cannot reasonably maintain an expectation of privacy in that which they display openly," regardless of "whether the observation of openly displayed facts is accomplished by a video camera or the naked eye" (quoting Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 181 (1st Cir. 1997))). *See generally* Katz v. United

positioned in plain view (making the surveillance open and obvious), when employees have consented to the surveillance, and when the employer has a legitimate business justification for the recording.[270]

One example is *Vega-Rodriguez v. Puerto Rico Telephone Co.*,[271] where the United States Court of Appeals for the First Circuit found it "implausible to suggest that society would recognize as reasonable an employee's expectation of privacy against being viewed . . . in the [employer's] open and undifferentiated work area."[272] In upholding this instance of video surveillance, the First Circuit also noted that the employer had a legitimate business interest for conducting the surveillance, and that the employer acted overtly by notifying its employees in advance that cameras would be installed and disclosing the cameras' field of vision.[273] According to the First Circuit, "[w]hen all is said and done, employees must accept some circumscription of their liberty as a condition of continued employment."[274]

Of course, one key difference between video surveillance in open areas and the contact tracing technologies discussed in Part I that utilize Bluetooth or similar technology is the ability of those technologies to capture data regarding the interactions of employees in *all parts* of the workplace, including private areas such as restrooms.[275] In the context of video surveillance, this distinction can make a difference.[276] Nevertheless, video surveillance in private areas is problematic precisely because it permits a *view* of the plaintiff in his or her private activities. This is not the case with contact tracing apps or wearables, which typically only capture data regarding employee interactions by recording their proximity and time spent interacting.[277]

Along with these video surveillance precedents, the contact tracing technologies described in Part I that rely on Bluetooth or Wi-Fi do not require access to the *contents* of an employee's cell phone, for which expectations of privacy are heightened.[278] As noted in *Port Authority* and similar cases,

States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

270. *See, e.g.*, Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174 (1st Cir. 1997).

271. 110 F.3d 174 (1st Cir. 1997).

272. *Id.* at 180.

273. *Id.*

274. *Id.*

275. *Cf. id.* at 181 (finding it significant that the employer's video cameras "do not pry behind closed office doors or into desks, drawers, file cabinets, or other enclosed spaces, but, rather, record only what is plainly visible on the surface").

276. *See* Koeppel v. Speirs, 808 N.W.2d 177, 182–84 (Iowa 2011) (discussing tort of intrusion cases involving secret videotaping of employees in private areas, such as restrooms).

277. *See supra* notes 49–57 (discussing the PwC contact tracing app).

278. *See* Riley v. California, 573 U.S. 373, 393–98 (2014). Fourth Amendment law generally recognizes a distinction between the contents of a communication (such as GroupMe chats) and the

employees generally have a legitimate expectation of privacy in the *contents* of their personally-owned cell phones.[279] Importantly, however, when an employer implements contact tracing through a cell phone app, this generally does not require the employer to search or otherwise access the contents of any employee-owned device, making the tracing less invasive.[280] The PwC tracing device, for example, simply requires workers to authorize contact tracing through an app on their cell phone.[281] Once installed, the PwC app runs in the background throughout the day and uses Bluetooth and Wi-Fi data to determine employees' proximity to one another and the amount of time employees spend interacting.[282] As a result, an employer's implementation of a contact tracing app would likely not infringe any reasonable expectation of privacy. For similar reasons, there could be no reasonable expectation of privacy in wearable contact tracing devices provided by an employer for the sole purpose of contact tracing because, unlike other wearable smart devices like fitness activity trackers, such contact tracing devices do not contain protected private information.[283]

In addition, unlike the GPS data and cell site location information ("CSLI") at issue in cases like *Jones* and *Carpenter v. United States*,[284]

addressing information associated with that communication (such as to whom a chat is directed). *See* Smith v. Maryland, 442 U.S. 735, 741–43 (1979). In the employment context, courts have recognized that it is generally more invasive to access the contents of employee communications, such as text messages, as opposed to a list of numbers and names with which a person has communicated. *See, e.g.*, McGreal v. AT&T Corp., 892 F. Supp. 2d 996, 1015 (N.D. Ill. 2012) (distinguishing between the contents of plaintiff's phone calls or text messages, which would be "extremely personal," and "[a] bare list of phone numbers," which "is not sufficiently private to meet the elements of an intrusion upon seclusion claim"); Cunningham v. Terrebonne Par. Consol. Gov't, No. 09-8046, 2011 WL 651997, at *2, *5 (E.D. La. Feb. 11, 2011) (rejecting summary judgment for employee on his Fourth Amendment claim due to genuine issues of fact as to whether the employee had a reasonable expectation of privacy in his cell phone records containing only numbers dialed and received, but not names or substance); Sunbelt Rentals, Inc. v. Victor, 43 F. Supp. 3d 1026, 1035 (N.D. Cal. 2014) ("This and other courts have concluded that there is no 'legally protected privacy interest and reasonable expectation of privacy' in electronic messages, 'in general.' Rather, a privacy interest can exist, if at all, only with respect to the content of those communications." (emphasis omitted) (citations omitted)).

279. *See* Port Auth. Police Benevolent Ass'n v. Port. Auth. of N.Y. & N.J., No. 15-CV-3526, 2017 WL 4403310, at *5 (S.D.N.Y. Sept. 29, 2017) (discussing the impact on public employers of *Riley v. California*, 573 U.S. 373 (2014)); Hibbert v. Schmitz, No. 3:16-CV-3028, 2017 WL 59075, at *5–6 (C.D. Ill. Jan. 5, 2017) (finding employee's complaint sufficiently alleged a search under the Fourth Amendment based on her employer's act of copying the personal information on her iPhone).

280. *See supra* note 278 and accompanying text.

281. Putzier & Cutter, *supra* note 3.

282. *See supra* note 51 and accompanying text.

283. *See* Katharine Saphner, *You Should Be Free to Talk the Talk and Walk the Walk: Applying* Riley v. California *to Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1691–92, 1706–10 (2016) (applying *Riley v. California* to data from smart wearable technology, such as activity trackers, and arguing that such digital data should generally be protected by the warrant requirement).

284. 138 S. Ct. 2206 (2018).

contact tracing apps and wearable contact tracing devices do not generate detailed location information, but instead only capture data regarding relative proximity to other devices, which is naturally less invasive.[285] Finally, as the Supreme Court has ruled in numerous cases, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[286] Under this doctrine, an employee who voluntarily turns over location data to his or her employer for the limited purpose of contact tracing would no longer have any expectation of privacy in that data, at least vis-à-vis the employer.

2. Physical Trespass Search Test

As an alternative to the *Katz* test, courts sometimes apply the physical trespass test to determine whether a Fourth Amendment "search" has occurred.[287] Under this test, a Fourth Amendment "search" occurs, irrespective of the *Katz* test, when the government physically trespasses on "persons, houses, papers, and effects" to obtain information.[288] Such a trespass occurs when a government agent, without consent, encroaches on an area or object protected by the Fourth Amendment, such as a person's vehicle or home, in order to find something or obtain information.[289]

Although an individual's personally-owned cell phone is undoubtedly an "effect" under the Fourth Amendment,[290] the physical trespass "search" test seemingly does not apply to the types of cell phone app-based contact tracing technologies described in Section I.B.2. For one, most employees who permit contact tracing through apps like the PwC app do so only after voluntarily consenting to that action, and there is no physical trespass in that

285. *See* United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (recognizing that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations"); *Carpenter*, 138 S. Ct. at 2211, 2216 (emphasizing that the CSLI data at issue "provide[d] a comprehensive chronicle of the user's past movements," and stating that the "[m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled").

286. *Carpenter*, 138 S. Ct. at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

287. *See supra* notes 141–143 and accompanying text.

288. U.S. CONST. amend. IV; *Jones*, 565 U.S. at 406–07, 407 n.3; *see also* Florida v. Jardines, 569 U.S. 1, 5 (2013); State v. Jean, 407 P.3d 524, 528 (Ariz. 2018).

289. *Jones*, 565 U.S. at 410; *Jardines*, 569 U.S. at 11; *id.* at 7–10 (discussing the lack of consent by Jardines).

290. *Cf. Jones*, 565 U.S. at 404 ("It is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment.").

instance.[291] But even assuming that such consent is coerced, the lack of any *physical intrusion* likely rules out the physical trespass test.[292]

As originally understood, the Fourth Amendment did not apply in the absence of a physical intrusion—a trespass—upon a constitutionally protected area.[293] And as the United States Supreme Court more recently noted in *Jones* and in *Florida v. Jardines*,[294] there must be an actual *physical intrusion* upon an individual's person, house, paper, or effect for a Fourth Amendment search to occur under this alternative search test.[295] In *Jones*, for example, police physically mounted a GPS receiver on the defendant's automobile, thus intruding on his "effect."[296] In *Jardines*, police physically intruded on Jardines' constitutionally protected property (his house) in order to gather evidence against him in a criminal investigation.[297] Here, by contrast, when an employee downloads an app to his or her cell phone, no such physical intrusion occurs.[298]

---

291. *See id.* at 408–10 (discussing the effect of consent upon a Fourth Amendment physical trespass claim); *see, e.g.*, El-Nahal v. Yassky, 993 F. Supp. 2d 460, 467–68 (S.D.N.Y. 2014) (finding no common law trespass and refusing to apply *Jones* to an employer's installation of a GPS tracking system in taxicabs), *aff'd*, 835 F.3d 248 (2d Cir. 2016); State v. Malloy, No. 20190446, 2021 WL 209290, at *5 (Utah 2021) ("A trespass is an unconsented physical 'intrusion' on a person's property. Such intrusion is effected when a police officer physically touches or impacts another person's property, as with the attachment of a GPS device to a car, or even 'an officer's momentary reaching into the interior of a vehicle.' There is no trespass, however, where the intrusion on property is effected through the consent or invitation of the property owner." (footnote omitted)).

292. *Cf. Jardines*, 569 U.S. at 7–10 (discussing Jardines' lack of consent).

293. *See* Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding no Fourth Amendment "search" occurred under the physical trespass test when officers used wiretaps installed on telephone lines outside Olmstead's property to intercept telephone conversations occurring inside because "[t]here was no entry of the houses or offices of the defendants"), *overruled in part by* Berger v. State, 388 U.S. 41 (1967), *and* Katz v. United States, 389 U.S. 347 (1967); Lopez v. United States, 373 U.S. 427, 438–39 (1963) (describing the Supreme Court's physical trespass cases involving electronic eavesdropping as "insist[ing] only that the electronic device not be planted by an unlawful physical invasion of a constitutionally protected area").

294. 569 U.S. 1 (2013).

295. *Jones*, 565 U.S. at 407 (reaffirming the principle "that, when the Government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment") (emphasis omitted) (quoting United States v. Knotts, 460 U.S. 276, 286 (1983)); *Jardines*, 569 U.S. at 11 ("That the officers learned what they learned only by physically intruding on Jardines' property to gather evidence is enough to establish that a search occurred."); *see also* State v. Phillips, 382 P.3d 133, 149 (Haw. 2016) (recognizing that "[u]nder the *Jones*/*Jardines* trespass-intrusion test, the first question is whether there is a trespass or physical intrusion to persons, houses, papers, or effects. A physical intrusion is the act of 'entering without permission'" (quoting BLACK'S LAW DICTIONARY 951 (10th ed. 2014)).

296. *See Jones*, 565 U.S. at 403 (explaining that "agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot").

297. *Jardines*, 569 U.S. at 11.

298. As explained, the *Jones* trespass doctrine would not apply unless the contact tracing app itself would be considered physically intrusive of the device. This is doubtful in light of the *Jones* Court's statement that "[s]ituations involving merely the transmission of electronic signals without

In the event an employee is *compelled* by her employer to don a wearable tracking device, such as a wearable GPS-enabled necklace, the case more closely resembles *Jones*.[299] In *Jones*, acting without a valid warrant, police officers surreptitiously attached a GPS tracking device to the undercarriage of suspect Antoine Jones's vehicle and used the device to track the vehicle for twenty-eight days.[300] In doing so without Jones's consent, the officers "physically occupied private property for the purpose of obtaining information," constituting a Fourth Amendment "search."[301]

In *Jones*, the Court emphasized that "[b]y attaching the device to the Jeep, officers encroached on a [constitutionally] protected area."[302] By analogy, if an employer attempts to collect location information by "attaching" a tracing device to an employee's "person"—a constitutionally protected area—a Fourth Amendment search would arguably occur.[303] If

trespass would remain subject to *Katz* analysis." 565 U.S. at 411 (emphasis omitted). Of course, one might argue that if an employer coerces its employees into downloading and activating the app, a physical trespass of the device might occur. *See, e.g.*, Hernandez v. Path, Inc., No. 12-CV-01515 YGR, 2012 WL 5194120, at *2, *7–8 (N.D. Cal. Oct. 19, 2012) (applying California trespass law and suggesting that a trespass to chattels might occur when a cell phone user downloads an app that is then used in a manner that exceeds the scope of the user's consent, but dismissing the claim because plaintiffs alleged the unauthorized action caused "depletion of 'two to three seconds of battery capacity,'" a *de minimis* injury). It is perhaps for this reason that Minnesota Law School Professor Alan Z. Rozenshtein has argued that "any government surveillance program that required individuals to download an app on their phones might constitute a Fourth Amendment search under the trespass test, since it would interfere in individuals' property interests—that is, to control what is on their devices." Rozenshtein, *supra* note 34. This view of trespass finds some support in the case law. *See, e.g.*, *In re* Apple & AT & TM Antitrust Litig., 596 F. Supp. 2d 1288, 1306–07 (N.D. Cal. 2008) (refusing to dismiss a trespass to chattels claim based on the plaintiffs' act of downloading software to their cell phones).

299. *See* Rozenshtein, *supra* note 34 (arguing that "[i]f the government required infected individuals to download a location-broadcasting app on their phones—or, in an extreme case, to wear a physical device, like a GPS bracelet—that would almost certainly trigger the Fourth Amendment under *Jones*").

300. *See Jones*, 565 U.S. at 403.

301. *See id.* at 404–05.

302. *Id.* at 410.

303. *See* U.S. CONST. amend. IV (guaranteeing "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"); *Jones*, 565 U.S. at 407 n.3 ("Where . . . the Government obtains information by physically intruding on a constitutionally protected area, such a [Fourth Amendment] search has undoubtedly occurred."); *id.* at 411 n.8 (stating that "[t]he Fourth Amendment protects against trespassory searches only with regard to those items ('persons, houses, papers, and effects') that it enumerates" (quoting U.S. CONST. amend. IV)); *see also* HON. GREGORY M. CASKEY, CAL. SEARCH & SEIZURE § 2:11 (2021) (recognizing that "[a] physical intrusion of a person for the purpose of obtaining information or evidence is a search" under *Jones*); *Cunningham II*, 997 N.E.2d 468, 471–72 (2013) (applying the *Jones* physical trespass test in the employment context to find a "search" had occurred when a public employer attached a GPS device to an employee's vehicle and used the device to monitor the vehicle's movements).

employees *consent* to the use of such wearables, however, which is the most likely scenario, no such trespass would occur.[304]

3. Seizure of the Employee's Person

Fourth Amendment claims may involve seizures of persons, which occur when there has been "a meaningful interference with [the person's] freedom of movement."[305] In the criminal investigation context, seizures of persons include arrests or de facto arrests,[306] and less intrusive investigative detentions known as "Terry-level" seizures.[307] For any type of Fourth Amendment seizure, the important point is that the individual's freedom of movement has been restrained.[308] In the instant context, however, when an employer utilizes a contact tracing device to track employee interactions (or even their locations), the employer does not meaningfully restrain the employees' freedom of movement.[309] Rather, employees can go about their day as usual, with the contact tracing technology working in the background, often completely unnoticed.[310] As such, no seizure of the employees themselves occurs.[311]

Of course, anytime a person is required to be in the workplace for a set period of time, that person would not generally feel "free to leave" the workplace during that window of time, perhaps suggesting that the

304. *See Jones*, 565 U.S. at 408–10 (distinguishing two prior Supreme Court opinions—*United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984)—on the basis of consent); *see also* Lopez v. United States, 373 U.S. 427, 438–39 (1963) (finding that no Fourth Amendment "search" occurred under the physical trespass test when an undercover agent consensually entered a criminal suspect's premises with a tape recorder because the invited agent was there "with petitioner's consent" and was not a trespasser).

305. Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 616 (1989). *See generally* United States v. Davis, 94 F.3d 1465, 1467–68 (10th Cir. 1996) (summarizing the types of Fourth Amendment seizures).

306. *See* New York v. Harris, 495 U.S. 14, 17–18 (1990) (involving an arrest); Dunaway v. New York, 442 U.S. 200, 206–16 (1979) (involving a detention later characterized as a de facto arrest, even though the suspect was told he was not under arrest).

307. *See* Terry v. Ohio, 392 U.S. 1, 20–22 (1968) (authorizing a brief, temporary seizure of a person suspected of committing a crime on the basis of reasonable, articulable suspicion).

308. *See id.* at 19 n.16 (stating that "[o]nly when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen may we conclude that a 'seizure' has occurred"); California v. Hodari D., 499 U.S. 621, 625 (1991) (applying the Terry definition of "seizure").

309. *See* Torres v. Madrid, 141 S. Ct. 989, 998 (2021) (recognizing that not "every physical contact between a government employee and a member of the public [amounts to] a Fourth Amendment seizure"; rather, "[a] seizure requires the use of force *with intent to restrain*").

310. *See supra* note 51 and accompanying text.

311. *Cf. Hodari D.*, 499 U.S. at 625–26 (holding that one type of seizure occurs when a criminal suspect submits to an officer's show of authority, thereby resulting in an actual restraint of the suspect's movement).

individual's freedom of movement is in fact restrained.[312] While this may be true, it is the fact of employment itself, coupled with the employer's general requirements specifying how and where the employee's work must be performed, that causes any such restraint.[313] The employer's contact tracing technology does not. Accordingly, it is doubtful that the mere implementation of a contact tracing program would constitute a seizure of an employee.

4. Seizure of the Employee's Property

The alternative seizure question is whether a seizure of employee property occurs when a contact tracing program is implemented. Under Fourth Amendment precedent, a seizure of property occurs "when there is some meaningful interference with an individual's possessory interests in that property."[314]

When an employee agrees to utilize a wearable contact tracing device provided by an employer, such as a smart necklace, there is no seizure of the *employee's* property.[315] The device itself is owned by the employer, rather than the employee, and the employee's sole possessory interest in the device is for contact tracing purposes in the manner defined by the employer, a possessory interest that is not "interfered" with by the employer.[316] Simply put, because the employee's possessory interest in the device is for contact tracing purposes only, there is no meaningful interference with that possessory interest when the device is used solely for that purpose.[317]

312. *See* I.N.S. v. Delgado, 466 U.S. 210, 218 (1984) (recognizing that "[o]rdinarily, when people are at work their freedom to move about has been meaningfully restricted, not by the actions of law enforcement officials, but by the workers' voluntary obligations to their employers"); Carter v. City of Milwaukee, 743 F.3d 540, 544 (7th Cir. 2014) (same); United States v. Mendenhall, 446 U.S. 544, 554 (1980) (stating that "a person has been 'seized' within the meaning of the Fourth Amendment only if, in view of all of the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave").

313. *See Delgado*, 466 U.S. at 218 (rejecting Fourth Amendment seizure claim brought by a group of employees who were detained for a brief period of time for questioning).

314. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

315. *Cf.* United States v. Karo, 468 U.S. 705, 711 (1984) (finding that no Fourth Amendment "seizure" occurred when DEA agents placed a beeper inside a can of ether that at the time belonged to the DEA); *id.* at 711–13 (rejecting the argument that a Fourth Amendment "seizure" occurred when the can of ether was later transferred to the defendant).

316. *See id.*; *cf.* State v. Jean, 407 P.3d 524, 528 (Ariz. 2018) (rejecting seizure argument based on warrantless GPS tracking of a truck because defendant himself, who was a passenger in the truck, did not own the truck and never possessed the truck outside of the owner's presence).

317. *Cf.* Tower v. City of Denton, No. 4:05CV302, 2007 WL 2900466, at *5 (E.D. Tex. Sept. 28, 2007) (refusing to grant summary judgment for the employer and its agents when the plaintiff-employee alleged that his briefcase and a locked metal box in his desk were searched in violation of the Fourth Amendment); O'Brien v. S. Suburban Coll., No. 93-C-7172, 1994 WL 376282, at *5 (N.D. Ill. July 15, 1994) (recognizing that an employee's purse "generally contains private property and personal items and effects, and generally is for the employee's exclusive use").

Alternatively, when an employee downloads a contact tracing app to his or her personal cell phone and enables the app to collect data of the phone's whereabouts, no seizure of the phone itself occurs.[318] Indeed, in this circumstance, there has been no meaningful interference with the employee's possessory interest in his or her device, as the employer has not exercised control over the device while denying control to the employee.[319] Rather, the right to possess the device remains at all times with the employee, who simply agrees to permit limited data collection by the employer through that device in a way that does not interfere with the phone's operation.[320]

Finally, no seizure of the employee's location data would occur in the context of contact tracing. First, unlike other types of seizable data such as emails or text messages, employees do not have a meaningful possessory interest in the record of who they came in close contact with at work, and thus have no real ownership interest in that data that could be "seized."[321] In addition, unlike GPS and CSLI data, contact tracing apps and wearables do not generate detailed location information; rather, such technologies only capture data that can be used to determine relative proximity to other devices, and it makes little sense to talk about a possessory interest in *that* type of data.[322] Finally, when an employee enables a cell phone app to allow for contact tracing data collection, the employer is not changing "the predetermined path of [that data] by some intentional action," as the data itself did not exist before this action.[323] Accordingly, it is unlikely that the Fourth Amendment would be implicated in this manner.

---

318. *See* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 705 (2010) (recognizing that "a seizure of physical property occurs when the government takes control of the property and denies control to others").

319. *See id.* at 711 (stating that "[i]n the case of movable property, property is seized when it is taken away from the person who has lawful control over it"); United States v. Jacobsen, 466 U.S. 109, 113 (1984); *cf.* Krivolenkov v. Ferrer, No. 3:20-CV-00759-MO, 2020 WL 6152360, at *5 (D. Or. Oct. 20, 2020) (finding police officer did not seize a suspect's cell phone simply by the act of a grabbing a suspect's wrist, causing the suspect to drop his phone on the ground).

320. *Cf.* United States v. Jones, 565 U.S. 400, 419 (2012) (Alito, J., concurring) (suggesting that a GPS device attached to a vehicle does not seize the vehicle under the Fourth Amendment because the device does "not interfere in any way with the operation of the vehicle").

321. *Cf.* Kerr, *supra* note 318, at 723–24 (discussing the interception of emails and the copying of remotely stored files as Fourth Amendment "seizures"); *see, e.g.*, Larios v. Lunardi, 445 F. Supp. 3d 778, 782 (E.D. Cal. 2020) (finding that employer's act of copying the entire contents of an employee's cell phone constituted a Fourth Amendment seizure); *In re* Search of Info. Associated with [Redacted]@mac.com, 13 F. Supp. 3d 145, 150 (D.D.C.) (declaring that "a seizure of property occurs when e-mails are copied and taken by the government without the owner's consent because an individual's 'possessory interest [in the e-mails] extends to both the original and any copies made from it'" (alteration in original) (quoting Kerr, *supra* note 318, at 703)), *vacated by* 13 F. Supp. 3d 157 (D.D.C. 2014).

322. *See supra* Section I.B.2 and I.C.

323. *See* Kerr, *supra* note 318, at 721.

C. Step 2: Reasonableness of Contact Tracing Methods

As discussed in the previous Section, any Fourth Amendment challenge to contact tracing conducted through cell phone apps or wearable devices would likely fail at the first step of Fourth Amendment analysis. Nevertheless, if employee consent to such surveillance is deemed coerced, such a finding might trigger Fourth Amendment protection. Accordingly, this Section assumes for the sake of analysis that the Fourth Amendment would apply, and thus considers whether the *O'Connor* workplace exception would permit such surveillance.[324]

Under *O'Connor*, a search or seizure must be both reasonable at its inception and reasonable in scope.[325] Importantly, however, the *O'Connor* workplace exception does not authorize *all* work-related intrusions. Rather, built into these standards is a requirement that the search be "work-related," or based on some legitimate employer interest.[326] In addition, as *O'Connor* notes, this exception applies only in the "workplace context," making the exception applicable only to "those areas and items that are related to work and . . . generally within the employer's control."[327] Accordingly, before applying the *O'Connor* reasonableness framework, one must first ensure the exception itself applies.

1. Applicability of O'Connor Workplace Exception

As noted, the *O'Connor* exception extends only to "those areas and items that are related to work and . . . generally within the employer's control."[328] Certainly, wearable tracking devices provided by the employer for the specific purpose of contact tracing within the workplace would encompass "items" (the wearables) and "areas" (the workplace) generally

324. Notably, if the *O'Connor* exception does not apply, a court would presumably apply a general Fourth Amendment reasonableness analysis that balances the competing interests at stake. *See* Riley v. California, 573 U.S. 373, 385, 393–98 (2014) ("Absent more precise guidance from the founding era, the Court generally determines whether to exempt a given type of search from the warrant requirement 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)). As discussed in Part IV, the same types of factors discussed in this Section remain relevant, including: (1) a legitimate business purpose underlying the employer's surveillance program; (2) employee consent to the surveillance program; and (3) surveillance that is limited to the workplace itself and does not capture data regarding off-duty movements. *See* Carniol v. N.Y.C. Taxi & Limousine Comm'n, 975 N.Y.S.2d 842, 848–49 (Sup. Ct. 2013), *aff'd*, 2 N.Y.S.3d 337 (App. Div. 2015).

325. O'Connor v. Ortega, 480 U.S. 709, 726 (1987).

326. *See, e.g.*, Ontario v. Quon, 560 U.S. 746 (2010).

327. *See O'Connor*, 480 U.S. at 715.

328. *See id.*

within the employer's control.[329] The more difficult question is whether employees' personal cell phones fall within the scope of this exception.

As cases like *Port Authority* recognize, employees' personal cell phones are not usually "items . . . related to work and . . . generally within the employer's control," and hence may not be subject to the *O'Connor* workplace exception.[330] Nevertheless, to the extent those devices are routinely used for a legitimate employment-related purpose—arguably including contact tracing—the *O'Connor* exception might apply. A 2020 United States district court case involving an employer's search of an employee's personal cell phone, *Larios v. Lunardi*,[331] supports this result.[332]

The plaintiff in that case, Timothy Larios, worked as a California Highway Patrol ("CHP") officer and served on the Shasta Interagency Narcotics Task Force ("SINTF"), where he often communicated with confidential informants.[333] SINTF policy declared that any CHP work product produced on personal devices, including personal cell phones, became the "property of the state and must be relinquished on demand."[334] During SINTF's investigation of a suspected marijuana dealer named Nathan Santana, Larios began a prohibited romantic relationship with a confidential informant involved in the investigation, Tawnya Mellow.[335] After Santana discovered a greeting card on Mellow's car from Larios that revealed his romantic feelings for her, prompting a domestic incident, Larios's employer began investigating his relationship with Mellow.[336] Investigators ordered Larios to produce his personal cell phone so they could determine the nature and extent of his interactions with Mellow.[337] Investigators then created a backup of Larios's entire phone and extracted all relevant text messages from that backup.[338]

329. *See Quon*, 560 U.S. at 760–62 (applying *O'Connor* to uphold an employer's search of text messages on an employer-issued pager); Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994) (finding no Fourth Amendment violation in the search of a judicial clerk's office, desk, and file cabinets, because clerk could not reasonably expect privacy in those areas).

330. *See O'Connor*, 480 U.S. at 715; *see also supra* notes 235–241 and accompanying text.

331. 442 F. Supp. 3d 1299 (E.D. Cal.), *determined by* 445 F. Supp. 3d 778 (E.D. Cal. 2020), *aff'd*, 856 F. App'x 704 (9th Cir. 2021).

332. *See Larios*, 445 F. Supp. 3d 778 (E.D. Cal. 2020) (analyzing the Fourth Amendment seizure issue); *Larios*, 442 F. Supp. 3d 1299 (E.D. Cal. 2020) (analyzing the Fourth Amendment search issue).

333. *Larios*, 442 F. Supp. 3d at 1302.

334. *Id.* at 1303 (quotation omitted). Larios received and reviewed this policy when he was a SINTF agent. *Id.*

335. *Id.* at 1302–03.

336. *Id.* at 1303.

337. *Id.* at 1304.

338. *Id.*

Larios later sued under the Fourth Amendment, alleging that the CHP Commissioner and officers involved in the search conducted an unlawful *seizure* when they downloaded the contents of his personal cell phone and an unlawful *search* when they inspected those contents.[339] On the search issue, the court noted that the *Larios* defendants had conducted an employee misconduct investigation in their capacity as supervisors, rather than a criminal investigation, with the goal of uncovering text messages that CHP considered "work product" under its governing policy.[340] Accordingly, the court determined that the *O'Connor* exception applied.[341]

Applying *O'Connor*'s two-part reasonableness test, the court first found that the defendants' "inspection of CHP work product" within Larios's phone was justified at its inception given that Larios had "inexplicably left a romantic greeting card at the residence of a confidential informant and the target of a criminal investigation," which jeopardized the case against Santana.[342] In searching Larios's text messages, CHP simply "sought to understand the scope of [Larios]'s communication with Mellow and mitigate harm that might flow from his potential misconduct," making the search reasonable at the outset.[343]

Regarding the scope of search, the court found that the "limited search of [Larios]'s texts with Mellow was reasonably related to the objectives of the investigation and not excessively intrusive given the grave abuse of power suspected."[344] The court emphasized that the defendants appropriately restricted their search to Larios's texts with Mellow, and even further "to a subset of [those] messages . . . from September 1, 2013 (the month Mellow initially contacted SINTF with information about Santana) to November 5, 2014 (the day before CHP directed [Larios] to produce his phone)," making the search reasonable in scope.[345]

The search conducted in *Larios* was done pursuant to an employer policy that made work product produced on personal devices the property of the employer that must be relinquished on demand.[346] This policy, in turn,

339. *Id.* at 1302.

340. *Id.*

341. *Id.* at 1309–10.

342. *Id.* at 1310.

343. *Id.*

344. *Id.* Although the court later found the defendants' *seizure* of the phone's *entire contents* separately unreasonable, see Larios v. Lunardi, 445 F. Supp. 3d 778, 785 (E.D. Cal. 2020), *aff'd*, 856 F. App'x 704 (9th Cir. 2021), the case is nevertheless significant in demonstrating how a properly limited *search* of a personal cell phone may fall within the parameters of the *O'Connor* exception.

345. Larios v. Lunardi, 442 F. Supp. 3d 1299, 1310 (E.D. Cal.), *determined by* 445 F. Supp. 3d 778 (E.D. Cal. 2020), *aff'd*, 856 F. App'x 704 (9th Cir. 2021).

346. *Id.* at 1303.

made these particular cell phone contents "related to work and . . . generally within the employer's control" under *O'Connor*.[347] By analogy, the data produced by a contact tracing app installed on an employee's cell phone could be lawfully inspected by the employer under the *O'Connor* workplace exception, especially when, as in *Larios*, the employee is aware that the data is subject to inspection by the employer. Moreover, with many contact tracing technologies, the tracing *data itself* always remains within the employer's control and, unlike *Larios*, need not be extracted from other private data contained within an employee's device.[348]

2. What Makes Contact Tracing Reasonable at the Outset

Assuming the *O'Connor* workplace exception applies, the first question under that exception is whether an employer's contact tracing program is reasonable at its inception.[349] According to *O'Connor*, a search by an employer will be *reasonable at its inception* when the employer has "reasonable grounds for suspecting" either "[(a)] that the search will turn up evidence that the employee is guilty of *work-related* misconduct, or [(b)] that the search is necessary for a noninvestigatory *work-related* purpose."[350] Because workplace-wide contact tracing would not ordinarily take place in the context of a misconduct investigation, an employer's contact tracing program must instead be necessary for a "noninvestigatory *work-related* purpose."[351]

Under this aspect of *O'Connor*, an employer should first ensure that its contact tracing program is necessary for a "noninvestigatory *work-related* purpose."[352] Stated differently, the employer must ensure that a legitimate business objective justifies such data-collection and surveillance.[353] As noted in the Introduction, many American employers have a legal obligation to provide a work environment "free from recognized hazards that are causing

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

348. *See* Larios v. Lunardi, 445 F. Supp. 3d 778, 785 (E.D. Cal. 2020) (rejecting the *O'Connor* exception as justification for seizing *all data* within an employee's cell phone, including both work product and personal data, as "[t]he volume of data . . . seized was vastly disproportionate to the amount of work product . . . on [the] phone"), *aff'd*, 856 F. App'x 704 (9th Cir. 2021).

349. *O'Connor*, 480 U.S. at 726.

350. *Id.* (emphasis added).

351. *Id.* (emphasis added).

352. *Id.* (emphasis added); *see, e.g.*, Ontario v. Quon, 560 U.S. 746, 761 (2010) (holding a City employer's search of employee text messages reasonable at its inception because the City had reasonable grounds for suspecting that the search was necessary to determine whether the character limit on its contract with Arch Wireless was sufficient).

353. *See id.* (holding that the City "had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand that the City was not paying for extensive personal communications").

or are likely to cause death or serious physical harm."[354] According to OSHA, COVID-19 falls within the scope of this law, and requires employers to take affirmative steps to reduce COVID-19 related hazards in the workplace.[355] Even for those employers not subject to the Occupational Safety and Health Act, which includes various public employers,[356] an employer's goal of minimizing COVID-19 infections amongst its workforce is most assuredly a legitimate business objective, particularly during a time when the virus is spreading or infection rates are high.[357] As *Carniol* recognized, ensuring the safety and well-being of employees and customers is a legitimate business purpose or "substantial" governmental interest.[358] If this is true of the taxi industry, it is certainly true for employers wishing to protect the lives of employees and maintain efficient business operations in a pandemic-stricken economy.[359] And as in *Carniol*, where the employer implemented GPS tracking to accomplish its legitimate business objective, the use of contact tracing technology is an efficient way of accomplishing these noninvestigatory objectives.[360]

Under a general Fourth Amendment reasonableness analysis, courts would ordinarily balance the degree to which the employer's intrusion is needed for the promotion of legitimate employer interests against the degree to which it invades employee privacy.[361] For contact tracing accomplished through cell phone apps and wearable devices provided by an employer, the degree of intrusion upon employee privacy is minimal. The PwC contact tracing app, for example, simply runs in the background and uses Bluetooth and Wi-Fi data to determine employees' proximity to one another and the amount of time employees spend interacting.[362] The app does not track

354. 29 U.S.C. § 654(a); *see also* Hoffman & Litchfield, *supra* note 1.

355. *See* OCCUPATIONAL SAFETY & HEALTH ADMIN., *supra* note 2, at 8–16 ; *see also* Hoffman & Litchfield, *supra* note 1.

356. *See supra* note 1.

357. *See* Carlie Porterfield, *Coronavirus Has Killed More Americans than Any Flu in Half a Century*, FORBES (Apr. 30, 2020, 12:17 PM), https://www.forbes.com/sites/carlieporterfield/2020/04/30/coronavirus-has-killed-more-americans-than-any-flu-in-half-a-century/?sh=46a9b9aa3d3c (reporting on the dangers of COVID-19).

358. *See supra* note 204 (discussing *Carniol*).

359. *See generally* O'Connor v. Ortega, 480 U.S. 709, 723 (1987) (recognizing that "[t]he governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace").

360. *See* Ramjee et al., *supra* note 21, at 103 (recognizing that "digital surveillance tools provide a potential opportunity to supplement existing contact tracing initiatives by facilitating the fast identification of known and unknown contacts").

361. *See supra* note 119.

362. *See supra* note 51 and accompanying text.

anyone's location or analyze data outside of work, making it less invasive than the type of round-the-clock surveillance conducted in *Cunningham*.[363]

Although such app-based contact tracing technologies are relatively unintrusive, obtaining employee consent for such surveillance will help ensure that an employer's program of contact tracing remains reasonable at the outset.[364] After all, if an employee understands that their movements and interactions at work will be monitored, a reasonable employee would be aware that sound management principles might require review of that data.[365] Accordingly, although employee consent is not categorically required by the Fourth Amendment, obtaining valid employee consent to the employer's program of contact tracing would tilt the reasonableness balancing even further in the employer's direction.[366]

3. Permissible Scope of Contact Tracing and Least Invasive Tracing Techniques

According to *O'Connor*, a search will be *reasonable in scope* when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive."[367] Under this standard, the underlying business justification for the search delineates its permissible scope.[368] With that underlying business justification in mind, an employer should collect the *minimal* information necessary to achieve its objective.[369]

When an employer implements a system of contact tracing in the workplace, the employer's core objective is to protect the health and safety of employees and other individuals in the workplace by identifying potential virus exposures in an efficient and cost-effective manner.[370] Although round-the-clock contact tracing is obviously more likely to identify every potential exposure to the COVID-19 virus, employers must be careful not to engage in surveillance that a court might find excessively intrusive.[371] And as a comparison between *Carniol* and *Cunningham* shows, surveillance that is

363. Putzier & Cutter, *supra* note 3; Combs, *supra* note 50.

364. *See* Ontario v. Quon, 560 U.S. 746, 762 (2010); *cf.* Carniol v. N.Y.C. Taxi & Limousine Comm'n, 975 N.Y.S.2d 842, 849 (Sup. Ct. 2013) (discussing the role of employee consent under the reasonableness prong of Fourth Amendment analysis), *aff'd*, 2 N.Y.S.3d 337 (N.Y. App. Div. 2015).

365. *See Quon*, 560 U.S. at 762 (making a similar point).

366. *See supra* note 133.

367. O'Connor v. Ortega, 480 U.S. 709, 726 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 342 (1985)).

368. *See supra* notes 159–163 and accompanying text.

369. *See Quon*, 560 U.S. at 761–63 (discussing the employer's limited scope of search); Larios v. Lunardi, 442 F. Supp. 3d 1299 (E.D. Cal.) (same), *determined by* 445 F. Supp. 3d 778 (E.D. Cal. 2020), *aff'd*, 856 F. App'x 704 (9th Cir. 2021).

370. *See supra* note 3.

371. *See O'Connor*, 480 U.S. at 726.

limited to the workplace itself and does not capture information regarding employees' off-duty whereabouts is far more likely to be upheld as reasonable.[372] Indeed, *Cunningham* determined that "[w]here an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable."[373] Accordingly, the least invasive contact tracing technologies are those that are limited in geographic scope to the workplace itself and limited in temporal scope to working hours.[374] The contact tracing cell phone apps and wearable devices discussed in Part I satisfy these standards.[375]

V. PROPOSALS AND UNDERLYING CONCERNS

Both app-based contact tracing and contact tracing accomplished by wearable devices are typically carried out for the noninvestigatory, work-related purpose of minimizing COVID-19 infections and ensuring the safety and well-being of employees and others in the workplace. In *O'Connor*, the Supreme Court declared that public employers should be afforded "wide latitude" to conduct such searches in order "[t]o ensure the efficient and proper operation of the agency."[376]

Despite the "wide latitude" afforded employers, relevant Fourth Amendment precedents reveal that employers should avoid engaging in excessively intrusive surveillance.[377] Accordingly, employers should opt for the contact tracing technologies that collect the minimal information necessary to accomplish the relevant employment objective.[378] This includes collecting data that is limited to the workplace itself, that does not encompass non-working hours, and that is anonymized to the maximum extent possible.[379] To ensure that any contact tracing program passes muster under the Fourth Amendment, employers should also notify employees of their contact tracing plans, obtain employee consent, and avoid a blanket rule

372. *See supra* Part III.

373. *Cunningham II*, 997 N.E.2d 468, 473 (2013).

374. This is generally true of the technologies discussed in Section I.B.2. and Section I.C.—i.e., contact tracing using cell phone Bluetooth data, and contact tracing accomplished through wearable location monitoring devices. *See* Barnes et al., *supra* note 9 (arguing that employers wishing to implement contact tracing apps should avoid gathering data from employees while off duty).

375. *See supra* text accompanying notes 361–363.

376. 480 U.S. at 723.

377. *See id.* at 723, 726; Ontario v. Quon, 560 U.S. 746, 761–63 (discussing the limited scope of the challenged search).

378. *See id.* at 723, 726; Ontario v. Quon, 560 U.S. 746, 761–63 (discussing the limited scope of the challenged search); *see also* Ramjee et al., *supra* note 21, at 105–06 (arguing that digital contact tracing tools should establish data collection and processing at a scale that is limited to what is minimally necessary for achieving specific public health objectives).

379. *See* Barnes et al., *supra* note 9.

requiring all employees to participate in contact tracing in order to alleviate any concerns over potentially coerced consent.[380]

Although the contact tracing apps and wearable contact tracing devices discussed in Sections I.B.2 and I.C would likely not violate the Fourth Amendment for the reasons outlined in the previous Part, the potential of certain contact tracing technologies to cast a wide net of surveillance requires careful analysis regarding whether certain tracing technologies could be deemed unreasonable on the whole.[381] In recent Fourth Amendment cases, the United States Supreme Court has recognized that individuals may reasonably expect privacy in the whole of their physical movements.[382] Because of this, the Supreme Court has deemed the warrantless, round-the-clock surveillance of a criminal suspect's movements unreasonable.[383] Lower courts have ruled the same.[384]

Beyond the criminal context, recent precedents reveal a Court concerned with the long-term, unrestrained tracking of ordinary law-abiding citizens with no suspicion of wrongdoing.[385] In striking down the warrantless gathering of over one hundred days of a suspect's CSLI in *Carpenter*, for example, the Supreme Court emphasized that the data at issue "provide[d] a

380. *See id.* (identifying these variables).

381. *See* Ramjee et al., *supra* note 21, at 126–27 (noting the possibility of "mission creep" where governments could extend the use of contact tracing apps beyond their intended purpose of disease control to enforce travel restrictions and quarantine orders, including imposition of fines and potential criminal charges (quoting Matthew Guariglia, *The Dangers of COVID-19 Surveillance Proposals to the Future of Protest*, ELEC. FRONTIER FOUND. (Apr. 29, 2020), https://www.eff.org/deeplinks/2020/04/some-covid-19-surveillance-proposals-could-harm-free-speech-after-covid-19 [https://perma.cc/PN7Y-JUSH])). Along these lines, Minnesota Law Professor Alan Z. Rozenshtein has argued that "[i]f . . . the government were to collect large amounts of location data from companies (in order to do contact tracing), that would likely trigger the Fourth Amendment under the *Katz* reasonable-expectation-of-privacy test." Rozenshtein, *supra* note 34.

382. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

383. In *Jones*, the Court unanimously struck down one instance of GPS tracking in which a suspect's vehicle was monitored on public streets for nearly a month. The Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search,'" thereby presumptively requiring a warrant. 565 U.S. 400, 404 (2012) (footnote omitted); *see also id.* at 430–31 (Alito, J., concurring) (concluding on behalf of Justices Alito, Ginsburg, Breyer, and Kagan that the lengthy GPS monitoring that occurred in that case constituted a Fourth Amendment "search," thereby presumptively requiring a warrant); *id.* at 413 (Sotomayor, J., concurring).

384. *See, e.g.*, State v. Jones, 903 N.W.2d 101, 113–14 (S.D. 2017) (ruling that the warrantless, long-term video recording of all activity outside a criminal suspect's home violated the Fourth Amendment); United States v. Senese, No. 18-CR-60076-BB, 2018 WL 3159733, at *7 (S.D. Fla. June 28, 2018) (finding that "[t]he warrantless placement and use of the GPS tracker on [a criminal suspect]'s vessel for 28 days . . . was an unreasonable search"), *aff'd*, 798 F. App'x 499 (11th Cir. 2020).

385. *See* McAllister, *supra* note 18 (discussing how *Jones* impacts employers).

comprehensive chronicle of the user's past movements,"[386] and noted that the "[m]uch like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled."[387] In light of these concerns, employers should avoid the more robust forms of contact tracing carried out through cell phone GPS,[388] or through other potentially more robust forms of location monitoring.[389]

CONCLUSION

At first blush, the idea of having one's movements traced at all times while at work, even for the noble cause of protecting the health and safety of others, might seem overly intrusive. Yet, for public employers, this Article has shown that the Fourth Amendment is likely not violated by the most common forms of contact tracing in use today, including cell phone app-based contact tracing technologies that rely on Bluetooth or Wi-Fi and wearable contact tracing devices that rely on similar technologies to determine workers' proximities to one another.

Nevertheless, the lessons learned from cases involving GPS tracking by employers tell a cautionary tale. Those cases reveal that when an employer considers implementing a program of contact tracing, the employer should opt for a contact tracing technology that collects the minimal information necessary to accomplish the employer's objective. This includes collecting data that is limited to the workplace itself, that does not encompass non-working hours, and that is anonymized to the maximum extent possible. As a best practice, the employer should also provide notice of the employer's contact tracing plans and obtain employee consent to such tracing without imposing a blanket rule requiring employee consent to alleviate any coercion-based concerns.

386. 138 S. Ct. at 2211.
387. *Id.* at 2216.
388. *See supra* Section I.B.1.
389. *See supra* Section I.E.