Marquette Benefits and Social Welfare Law Review

Volume 20
Issue 2 *Spring*

Article 7

2019

Comment: Microchipping Employees and Privacy Implications - Does My Boss Know Where I am Right Now?

Samuel E. Simpson

MICROCHIPPING EMPLOYEES AND PRIVACY IMPLICATIONS - DOES MY BOSS KNOW WHERE I AM RIGHT NOW?

Samuel E. Simpson[*]

Existing law surrounding employee privacy does not adequately address privacy concerns raised by microchip programs. A handful of states have passed laws that prohibit mandatory employee microchipping programs, but the vast majority have not passed any preventative legislation. In states that have passed laws, the limited protections that do exist fail to address a wide range of issues that have not yet come up in the context of employer-provided technology. This comment will briefly overview employee privacy law to highlight some of the issues that will arise if the law remains untouched. Then, it will propose solutions that would serve to better protect employees from these issues. As technology continues to develop, it will gather more information and the potential for abuse will only increase. Without legal safeguards, employees will be left nearly defenseless against employers with access to ever-increasing information about their employees.

[*] J.D. Candidate 2019, Marquette University Law School.

TABLE OF CONTENTS

I. INTRODUCTION

A company in Wisconsin[1] became the first company in the United States to launch a voluntary microchip program for its employees.[2] The company implants a chip the size of a grain of rice under an employee's skin, allowing quick computer access, building access, and the ability to use vending machines without cash.[3] While the idea of implanting a microchip under a person's skin is not new, even having appeared in movies or television shows,[4] its presence in the news raises questions about the privacy implications of this technology, especially in the employer-employee context. Because the microchip essentially becomes part of the employee's person, it raises privacy implications that have not yet been considered in the context of more traditional employer owned technology such as phones or computers. As technology continues to develop, courts and legislatures will need to address the new privacy concerns that implanted technology will raise in the workplace.[5]

II. RFID: AN OLD TECHNOLOGY WITH NEW APPLICATIONS

A. Historical Applications

Radio Frequency Identification (RFID) Technology has its roots in World War II where it was used by British forces to signal that an incoming plane belonged to an ally.[6] RFID Technology continued to develop and can be classified as either passive or active.[7] The difference between an active and a

---

1. Press Release, Three Square Market, *Three Square Market Microchips Employees Company-Wide* (July 20, 2017), https://www.prlog.org/12653576-three-square-market-microchips-employees-company-wide.html [hereinafter *Three Square Market*].

2. *Microchipped Employees: Wave of the Future?*, WISCONSIN LAWYER (Sept. 2017), https://www.wisbar.org/NewsPublications/WisconsinLawyer/Pages/Article.aspx?Volume=90&Issue=8&ArticleID=25827. [hereinafter *Microchipped Employees*].

3. *Id.*

4. *See, e.g.*, NCIS: NATURE OF THE BEAST (CBS television broadcast Sep. 20, 2011).

5. For some books that discuss privacy in a broad context, *see generally* JOHN D.R. CRAIG, PRIVACY AND EMPLOYMENT LAW (1999); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010); RAYMOND WACKS, PRIVACY: A VERY SHORT INTRODUCTION (2010).

6. Mark Roberti, *The History of RFID Technology*, RFID JOURNAL (Jan. 16, 2005), https://perma.cc/ZH9U-4XTS.

7. *Id.*

passive RFID microchip is that a passive chip can only send information to a reader that provides energy to the chip for that purpose.[8] An active RFID chip contains a transponder that has its own power source.[9] This can be a battery or even photovoltaic cells that capture energy from light.[10] Because an active RFID chip has its own power source, it often has the ability to send more data and from a farther distance compared to a passive RFID microchip.[11]

Passive technology only responds when a signal is sent by a transponder while active RFID broadcasts a signal.[12] RFID technology has been used for a variety of purposes including tracking nuclear waste, unlocking doors, and managing large herds of cows.[13] The RFID technology used in cows is the predecessor for the type of RFID technology that dog owners use to track lost dogs and that employers are now considering using with their employees.[14] In 2004, VeriChip Corporation developed the first chip cleared by the Food and Drug Administration (FDA) to be implanted in humans with the purpose of storing medical records for those with chronic illnesses that may make them unresponsive in a crisis.[15] Strong sales never materialized,[16] and use of the microchip in an employment context did not exist in the United States until 2017.[17]

B. Modern Applications

Beginning August 1, 2017, employees at Three Square Market (32M)[18] had the opportunity to get an RFID microchip implanted on a voluntary basis, making it the first company in the United States to start a program that would provide

8. *Id.*

9. Bob Violino, *The Basics of RFID Technology*, RFID JOURNAL (Jan. 16, 2005), https://www.rfidjournal.com/articles/view?1337.

10. *Id.*

11. *Id.*

12. *Id.*

13. Roberti, *supra* note 6.

14. *See generally* Roberti, *supra* note 6.

15. Anthony P. Gatto, *Under the Human Skin: Will Human Microchipping Prove to Be a Survivor in the Courtroom Just as DNA Evidence Did?*, 16 J. HIGH TECH. L. 409, 4442 (2016).

16. *Id.* at 443.

17. *See generally, Three Square Market, supra* note 1.

18. 32M is a company based in River Falls, Wisconsin. *Three Square Market, supra* note 1.

implanted microchip technology to its employees.[19] More than fifty employees volunteered to get a microchip implanted at 32M.[20] The purpose of the chip, as described by 32M, is to allow "employees to access the building and other facilities, quickly log in to computers, or purchase snacks without a wallet."[21] The company, which creates "micro markets" in company breakrooms and in prisons, sees advancements in implanted RFID microchips as one way to make using a micro market's services more convenient for its customers.[22] The company also claims there is potential for expanded use in the future to do other things such as unlocking phones, trading business cards, widespread use as a payment method, or even replacing your passport,[23] which is not completely unrealistic because RFID technology has already been used in United States passports since 2006.[24]

While 32M stands alone in the United States, it is not the first employer in the world to implement an implanted RFID microchip program in the workplace. Companies in Sweden and Belgium[25] have been using implanted RFID microchips with their employees, some as early as 2015.[26] BioHax is a Swedish company that has specialized in implanted microchips and has partnered with 32M to provide implanted chips to grow 32M's market share.[27] It was BioHax that gave 32M the idea to use implanted microchip technology as another payment option for its micro markets.[28]

Another Swedish company that has more recently implemented an implanted RFID microchip program is

---

19. *Three Square Market, supra* note 1.

20. *Three Square Market, supra* note 1.

21. *Microchipped Employees, supra* note 2.

22. *Three Square Market, supra* note 1.

23. *Three Square Market, supra* note 1.

24. Gatto, *supra* note 15.

25. NewFusion is a marketing firm in Belgium that has implemented an implantable microchip program with the same features as those that the Swedish Company Epicenter uses. Primarily, the purpose is to replace existing security cards with a chip that cannot be easily lost or forgotten. They are using the same company that Epicenter used to implement its microchip program. Tim Collins, *Would YOU let your boss implant you with a microchip? Belgian firm offers to turn staff into cyborgs to replace ID cards*, DAILY MAIL (Feb. 8, 2017), http://www.dailymail.co.uk/sciencetech/article-4203148/Company-offers-RFID-microchip-implants-replace-ID-cards.html.

26. *Microchipped Employees, supra* note 2.

27. *Three Square Market, supra* note 1.

28. *Three Square Market, supra* note 1.

Epicenter, a company based in Stockholm.[29] The company uses its RFID microchip program to achieve similar goals to those stated by 32M such as to "replace key cards, employee badges and credit cards for certain functions at the facility with technology that can't be lost or left behind."[30] Epicenter has had 75 of its 2000 employees volunteer to be chipped, and the company has stressed that these are passive chips with no more function than that of key cards with RFID chips.[31] While the implanted RFID chips have a limited purpose and abilities as they are used today, several questions remain, such as, what untapped abilities are available now that could be used if an employer wanted to have that function, and what the microchips might be capable of doing with further development.

The passive chips currently in use do not have the ability to track a user's location in real time, nor do they have the ability to track a user's location while not on the work premises.[32] Nevertheless, there are ways that the microchips can paint a picture of where someone has been throughout a workday.[33] For example, employees that work in an office may need to use their microchips to access the office, open doors within the office, make purchases in the break room, log onto their computer, use the printer, and anything else that employers currently require a badge swipe to do. Assuming all those sensors keep a log of swipes, over the course of a work day a supervisor can look at the logs to determine where that employee has been and what they are doing. While possession of this information from a single instance may not seem intrusive, over time it can help a supervisor make inferences and discover patterns in your daily routine that many people would find unsettling. These could be how many times you use the bathroom in a work-week, how many times you run to the breakroom to get a snack in the vending machine, or how frequently a smoker takes a smoke break. Once the information is gathered, it would be left to the discretion of the supervisor to either not use the information or

---

29. Jena McGregor, *Some Swedish workers are getting microchips implanted in their hands*, WASH. POST (Apr. 4, 2017), https://www.washingtonpost.com/news/on-leadership/wp/2017/04/04/some-swedish-workers-are-getting-microchips-implanted-in-their-hands/?utm_term=.9f659b1c75d7.

30. *Id.*

31. *Id.*

32. Dina Spector, *Microchips Will Be Implanted into Healthy People Sooner Than You Think*, BUSINESS INSIDER (Aug. 9, 2014), http://www.businessinsider.com/microchip-implants-in-healthy-people-2014-7.

33. *See, id.*

limit its use to ethical reasons only.

C. Development and Future Potential

Two potential uses of microchips should cause employees to proceed with caution in getting microchips, to ensure that the chips they receive have limited capabilities. The first is GPS tracking abilities. RFID chips that are in use by employers are currently passive chips.[34] While passive chips cannot be used as a GPS tracker, it is not outside of the realm of possibility that active RFID chips could be implemented that would have the ability to track the user via GPS.[35] Despite being passive in nature, the way that a company uses the chips could still allow supervisors to track employees with some level of accuracy as to their location while at work. Unlike the chips currently in use, active RFID microchips would provide real time data to whomever had access to the chip and the database system used to manage them.[36] The second use that might give pause is the ability to monitor blood sugar levels in diabetics.[37] These passive chips can give a glucose reading by scanning it with a reader, which is of great benefit for diabetics but illustrates the potential of the chips.[38] Employers could use the devices to monitor drug use or any number of health conditions. The potential implications are even more complicated if a government employer is monitoring a chip with this function and it determines the employee has been using illegal drugs.

While not an exhaustive list of the current or future capabilities of microchips, the above-mentioned possibilities illustrate potential uses by employers in a variety of contexts. If active chips are used in employees, what would prevent an employer from observing your every movement at all hours of the day? If the chips are only passive, that would prevent the employer from getting the data in real time but would not stop them from obtaining data stored on the device the next time an

---

34. Maggie Astor, *Microchip Imlants for Emplpoyee? One Company Says Yes,* N.Y. TIMES (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html.

35. Mark Roberti, *How Does RFID Monitor Employees?*, RFID JOURNAL (Aug. 19, 2005), https://www.rfidjournal.com/blogs/experts/entry?11501.

36. *Id.*

37.*Glucose-Sensing RFID Microchip*, DIABETES IN CONTROL (Dec. 5, 2006), http://www.diabetesincontrol.com/glucose-sensing-rfid-microchip/.

38. *Id.*

employee used it to open a door at work. If the sensors can detect blood sugar levels, what would prevent the development of chips that can sense other medical conditions, blood alcohol content, or even drug use. All an employer would need to do is calibrate the chips to also send that information every time the chip is used to log into a computer or pass through a door. Further, it is not easy to predict what an employer might do if they gain access to this information. The uncertainty surrounding employers' new-found access to employees' personal information raises concerns of employee privacy. If an employee elects to have an employer-provided microchip installed, questions as to what privacy rights that employee would have in the information contained within the microchip would arise.

Employees currently have limited privacy rights in the United States. Broadly, those rights can be divided into off-duty and on-duty interest, and different standards are applied to determine when there has been a violation of public employees privacy rights when compared to private employees privacy rights.[39] The rights that do exist are limited, in part, because most employees in the United States are by default considered employees at-will,[40] and most employees do not participate in a labor union that would give them the bargaining power to negotiate for additional protections.[41] That limited nature of employee privacy rights is concerning because of the increasing level of access employers have through work-provided computers and phones, and the ability to learn much that was once private through the growth of social media.[42] It becomes alarming, however, when the context becomes technology that becomes a part of you; technology that you cannot simply leave at home or in the office.

---

39. Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. 277, 278 (2012).

40. *See* Michael Z. Green, *Opposing Excessive Use of Employer Bargaining Power in Mandatory Arbitration Agreements Through Collective Employee Actions*, 10 TEX. WESLEYAN L. REV. 77, 89, 92, 95 (2003). This article discusses the lack of bargaining power in the employment at will context and how that weakens employees' ability to avoid unwanted arbitration agreements. This same lack of bargaining power would limit an employee's ability to avoid unwanted microchipping programs. There is further discussion of this idea later in the article.

41. *See* Press Release, U.S. DEP'T OF LABOR, *Union Members Summary* (Jan. 18, 2019), https://www.bls.gov/news.release/union2.nr0.htm, ("The union membership rate—the percent of wage and salary workers who were members of unions—was 10.5 percent in 2018").

42. *Social Media Factsheet*, PEW RESEARCH CTR. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/social-media/.

This comment will examine existing law surrounding employee privacy in general and the laws that exist surrounding employee microchipping programs. The comment will then recommend protections that should be put in place by building on the themes of employee privacy law in the United States - specifically Wisconsin - and by looking towards causes of action that already exist in the Restatement (Second) of Torts and the Restatement (Third) of Employment Law, and how those might be options to fill in the gaps of the current state of employee privacy law.

III. EMPLOYEE PRIVACY PROTECTIONS IN A NUTSHELL

A. Private Sector Employees

Private sector employees may be able to vindicate their privacy rights through the tort of Intrusion Upon Seclusion.[43] Specifically, the Restatement provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[44] One example of intrusion upon seclusion is illustrated in *K-Mart Corp. Store No. 7441 v. Trotti*,[45] a Texas tort case for invasion to privacy that has substantially similar requirements as the version in the Restatement (Second) of Torts.[46] *Trotti* involves a K-Mart employee and their work-provided locker.[47] K-mart provided their employees with work provided lockers where the employees could store their personal items while working.[48] The employees could use their own locks, or they could request a work-provided lock with the understanding that K-Mart would keep a copy of the combination or a key.[49]

---

43. Restatement (Second) of Torts § 652A (AM. LAW INST. 1977). The other privacy torts covered in this section – misappropriation of another's name and false light – are beyond the scope of this comment.

44. Restatement (Second) of Torts § 652B (AM. LAW INST. 1977). Only a small number of jurisdictions within the United States do not apply some form of the intrusion upon seclusion tort. *See generally,* Secunda, *supra* note 39.

45. K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632 (Tex. App. 1984).

46. *Id.*

47. *Id.* at 634.

48. *Id.*

49. *Id.*

On one occasion, an employee placed her purse in the locker and began her shift, but upon returning to the locker during an afternoon break, found the lock hanging open and her personal items in disorder.[50] Nothing was missing from the locker, but the employee had used her own lock and had locked the locker prior to the start of her shift.[51] When the employee approached her manager about whether the lockers or her purse had been searched, the manager initially denied either search.[52] This denial lasted for about a month before the manager admitted to conducting the search of both the locker and the purse, although the manager later stated that they had only searched the locker itself, and not the purse.[53]

The employee sued K-Mart for invasion of privacy and was able to obtain sizable damages.[54] While the specific issue in this case causing remand dealt with an issue of jury instructions, the case makes it clear that there is an action for the invasion of privacy in Texas.[55] In Texas, "an actionable invasion of privacy by intrusion must consist of an unjustified intrusion of the plaintiff's solitude or seclusion of such magnitude as to cause an ordinary individual to feel severely offended, humiliated, or outraged."[56]

The second question raised on appeal in *Trotti* was whether the evidence was sufficient to support the jury's verdict.[57] The court found there was sufficient evidence to support the jury's finding of an invasion of the employee's privacy.[58] It was significant to the court that the employee had "locked the locker with her own lock" "at the employee's own expense and with the [employer's] consent."[59] The court indicates the outcome might have been different had the employee used the employer-provided lock or had there been no lock at all because in either

50. *Id.* at 635.
51. *Id.*
52. *Id.*
53. *Id.*
54. Trotti was able to secure an award for $8,000 in actual damages and $100,000 in exemplary damages. *Id.* at 634.
55. *Id.* at 635. After this case was decided in the Court of Appeals of Texas, the Supreme Court of Texas denied an Application for a Writ of Error. Trotti v. K-Mart Corp. No. 7441, 686 S.W.2d 593 (Tex. 1985). The history of the case ends after the Writ of Error was denied.
56. *Trotti*, 677 S.W.2d at 636.
57. *Id.* at 637.
58. *Id.* at 638.
59. *Id.* at 637-38.

situation, the employers would have "manifested an interest both in maintaining control over the locker and in conducting legitimate, reasonable searches."[60] Because the employee used their own lock on the locker, the court determined there was enough evidence to support the jury's finding and survive appellate review for insufficient evidence.[61]

B. Public Sector Employees

Public employees have certain privacy rights at work, but those rights were not considered by the Supreme Court until 1987 in *O'Connor v. Ortega*.[62] Public sector employees generally have greater privacy rights than private sector employees.[63] In *O'Connor*,[64] the Court found that public sector employees may have a reasonable expectation of privacy in their place of work.[65] Dr. Ortega brought suit under 42 U.S.C. § 1983 for violation of his Fourth Amendment rights after he was terminated for mismanagement of the residency program at a state university.[66] As part of the investigation into his management of the residency program, hospital employees conducted a search of Dr. Ortega's office.[67] Although a thorough search was conducted, no formal inventory of the contents of the office was ever made.[68] The Court was tasked with deciding two issues: (1) whether a public employee "had a reasonable expectation of privacy in his office, desk, and file cabinets at his place of work"; and (2) if a reasonable expectation of privacy existed, what "the appropriate Fourth Amendment standard for a search" should be.[69]

First, the Court determined that it is possible for an employee to have a reasonable expectation of privacy in the workplace.[70] Courts must look towards "[t]he operational realities of the workplace" when determining reasonableness because in some circumstances, there might not be a reasonable

60. *Id.* at 637.
61. *Id.*
62. O'Connor v. Ortega, 480 U.S. 709 (1987).
63. *See* Paul F. Gerhart, *Employee Privacy Rights in the United States*, 17 COMP. LAB. L.J. 175, 176 (1995).
64. *O'Connor*, 480 U.S. at 709.
65. *Id.* at 717.
66. *Id.* at 712-14.
67. *Id.* at 713.
68. *Id.* at 712-714.
69. *Id.* at 711-712.
70. *Id.* at 717.

expectation of privacy "when an intrusion is by a supervisor rather than a law enforcement official.[71] In *O'Connor*, the Court determined that the doctor had a reasonable expectation of privacy in his desk and file cabinets.[72] The Court pointed to facts that support this conclusion, which included Dr. Ortega's exclusive use of the desk and file cabinets, his length of occupancy in that space, and the mix of personal and professional materials kept in the office.[73] Because there was a reasonable expectation of privacy in *O'Connor*, the court had to determine what the appropriate Fourth Amendment Standard should be.

When a search is conducted for "non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, [that search] should be judged by the standard of reasonableness under all the circumstances."[74] "Under this reasonableness standard, both the inception and the scope of the intrusion must be reasonable."[75] The Supreme Court did not decide whether the search was reasonable, but rather remanded the issue to the district court.[76] A majority of the Court did conclude that a warrant and probable-cause requirement would not be practical in the context of government employment.[77]

The Court took up the issue of public employee privacy again in *City of Ontario v. Quon*,[78] where the Court held that a search of an employer-provided beeper was reasonable because it was "motivated by a legitimate work-related purpose, and because it was not excessive in scope."[79] The City of Ontario issued pagers to the members of its SWAT team to help decrease response time in case of an emergency.[80] The pagers were allotted a limited number of characters each month but after the first few overages, it was suggested that SWAT members could reimburse the city for the overage.[81] Prior to disbursement, the city provided a computer policy that did not expressly include

71. *Id.*
72. *Id.* at 718.
73. *Id.*
74. *Id.* at 726.
75. *Id.*
76. *Id.* at 729.
77. *Id.* at 725, 732.
78. City of Ontario v. Quon, 560 U.S. 746 (2010).
79. *Id.* at 764. This case is important in the area of employee privacy law, which is why there is a lengthy discussion.
80. *Id.* 750-52.
81. *Id.* at 752.

text messaging but Quon was told in person that the pagers were considered email and could be audited, although it was also mentioned that there was no intention to audit the messages to determine if the overages were the result of work related messages.[82]

After several months of overages, the supervisor decided to investigate and see if the character limit needed to be revised because of the overages that were regularly incurred by Quon and another officer.[83] The supervisor reviewed transcripts of the messages and discovered that many messages that were sent or received were personal in nature, including some that were sexually explicit.[84] The matter was then referred to internal affairs.[85] Internal affairs redacted the messages that were sent or received outside of Quon's work schedule.[86] Internal affairs determined that Quon sent 456 messages during a workweek, of which only 57 were work related.[87]

"The Fourth Amendment applies . . . when the Government acts in its capacity as an employer."[88] In *Quon*, the Court elevated Justice Scalia's concurrence in *O'Connor* by analyzing *Quon's* Fourth Amendment claims against the City of Ontario through both the two-step analysis of the plurality in *O'Connor* and through Justice Scalia's concurrence.[89] The plurality's approach is to first determine if there is a reasonable expectation of privacy based on "[t]he operational realities of the workplace"; and second, if there is a reasonable expectation, it "should be judged by the standard of reasonableness under all of the circumstances" so long as the intrusion was either for non-investigatory work-related purposes or for investigations of work-related misconduct.[90]

Justice Scalia's approach differs from the plurality's in that it does not consider the operational realities of the workplace, but instead applies the Fourth Amendment as a general matter. It also differs because Justice Scalia would have held that a search that would be "reasonable and normal in the private-

82. *Id.*
83. *Id.*
84. *Id.* at 752-53.
85. *Id.* at 753.
86. *Id.*
87. *Id.*
88. *Id.* at 756 (citing Treasury Employees v. Von Raab, 49 U.S. 656, 665 (1989)).
89. *Id.* at 756-757.
90. *Id.*

employer context . . . do[es] not violate the Fourth Amendment."[91] In *Quon*, the Court declined to resolve the dispute because the outcome was deemed to be the same under either standard.[92]

The Court declined to determine if the employee had a reasonable expectation of privacy in the text messages sent on the beeper because even if he did, the audit of the messages was reasonable and the Fourth Amendment rights were not violated.[93] Under the plurality approach, the search was reasonable at the outset because it was done for a non-investigatory, work-related purpose—namely to determine whether the department needed to increase its character limit.[94] Further, the search was reasonable in scope because 1) it was a quick way to determine if the overages were caused by official activity, 2) the messages sent while Quon was off duty were redacted, and 3) the messages were only reviewed for some of the months of the program.[95]

Under Justice Scalia's approach, the search would be reasonable and normal in the private employer context because "a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used."[96] Therefore, in *Quon*, the search was reasonable, and the public employer did not violate Quon's Fourth Amendment rights.[97]

Since *Quon*, the Supreme Court has not heard another case to decide whether the plurality approach or Justice Scalia's approach from *O'Connor* controls. It is unclear what the Court would do in a situation where one standard is met, but not the other. Further, the Court operated under the assumption that there was a reasonable expectation of privacy in the beeper because that question was not outcome determinative,[98] therefore, it is unclear whether a public employee has a

---

91. *Id.* at 757.
92. *Id.*
93. *Id.* at 760.
94. *Id.* at 761.
95. *Id.* at 761-762.
96. *Id.* at 762.
97. *Id.* at 765.
98. *Id.* at 760. For further discussions on the impact of *Quon*, see Sheila A. Bentzen, *Safe for Work? Analyzing the Supreme Court's Standard Of Privacy for Government Employees In Light Of City Of Ontario V. Quon*, 97 IOWA L. REV. 1283 (2012); Franklin G. Shuler Jr. & Michelle Clayton, *When is Private Really Private? Privacy Interests in Employment After* Quon, 53(6) DRI FOR DEF. 61 (2011).

reasonable expectation of privacy in the messages they send on an employer-provided device.

Recently, public employees were said to have a greater privacy intertest at their place of employment than private sector employees, but scholars are noting that the difference is less clear than it was at one point in time.[99] Because the Court declined to choose between the two approaches in *Quon*, it remains unclear if the Court will move towards the approach used by Justice Scalia, which would make public employees' privacy rights incredibly similar to those of private sector employees.[100]

The cases have some overarching similarities that are worthy of note. The first is that these cases were primarily decided in the mid-1980s. The relative youth of these cases is problematic because they establish privacy interest recently enough that they cannot easily be defended by notions of history and tradition, yet they were decided before anyone could even imagine employers using technology that would be implanted under the skin of its employees as is the case with 32M. The rights that do exist are fairly limited in scope. You can only enforce an intrusion upon seclusion claim if it reaches the level of highly offensive to a reasonable person, meaning there is no redress if it is merely the normal amount of offensive.[101] In public sector employment, while privacy interests relate back to the Fourth Amendment to some extent, the law does not require government employers to obtain a warrant to conduct a search, but rather considers things such as the operational realities of the workplace.[102]

The limited scope of employee privacy rights is concerning against the backdrop of extensive personal information microchips have the potential to reveal, especially location and information about bodily functions. The concern with employer abuse is only amplified when paired with the grossly unequal bargaining power in the employee-employer relationship. Courts have been less reluctant to find that more traditional ideas of the freedom to contract are disappearing in the employer-employee context because of the disparity of bargaining

99. Secunda, *supra* note 39, at 277.

100. *Id.* at 294.

101. *See* K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 637 (Tex. App. 1984).

102. O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

power.[103] The disparity in bargaining power is caused by numerous factors that, when working together, make the employee more dependent on the employer than the employer is on the employee.

One major cause is the current "employment-at-will" context which exists in nearly every jurisdiction within the United States and allows employees to be fired for "good reason, a bad reason, or no reason at all."[104] While it is true that employment-at-will provides an employee relative freedom to leave one job for another, most workers live in families that operate on a paycheck-to-paycheck basis.[105] This means that the employee likely cannot afford to leave a job on a whim because there are little or no cash reserves to cover a period of unemployment.[106] An employee, even one with the financial difficulties previously mentioned, can leave if they have secured another job, but there are also challenges inherent in finding new employment.[107]

Another cause of unequal bargaining power is the general decline of union strength, especially in the private sector. The number of union employees has gone down by 2.9 million from 1983 until 2015, even though the number of jobs in the United States' economy have grown from 88.3 million to 133.7 million in that same period.[108] The result is that union participation has dropped from 20.1% to 11.1% in just over 20 years.[109] This is

---

103. Howard C. Ellis, *Employment-at-Will and Contract Principles: The Paradigm of Pennsylvania*, 96 DICK. L. REV. 595, 612 (1992). In the context of an employment contract where the question is whether the employee was an employee at will or had some other job questions, the author argues that Pennsylvania state courts are more willing to recognize some protection from at will employment when there is clear evidence to support it.

104. Green, *supra* note 40, at 77.

105. In August of 2017, CNBC reported that 78% of families live paycheck to paycheck. Even 10% of high income individuals, those who make more than $100,000, reported living paycheck to paycheck. Jessica Dickler, *Most Americans live paycheck to paycheck*, CNBC (Aug. 24, 2017), https://www.cnbc.com/2017/08/24/most-americans-live-paycheck-to-paycheck.html.

106. 56% of families save less than $100 per month. *Id.*

107. In 2015, Time reported that it takes an average of forty-three days to secure a job, although that figure largely depends on the industry in which you are employed. Healthcare workers have an average job search of sixty-five days. Martha C. White, *Here's How Long It Really Takes to Get a Job*, TIME (Oct. 22, 2015), http://time.com/money/4053899/how-long-it-takes-to-get-hired/.

108. Megan Dunn and James Walker, *Union Membership in The United States* (Sept. 2016), https://www.bls.gov/spotlight/2016/union-membership-in-the-united-states/pdf/union-membership-in-the-united-states.pdf.

109. *Id.*

particularly problematic because some have argued that collective action is one of the more likely methods to succeed for employees attempting to equalize bargaining power between employers and employees.[110] Union strength has been tested in recent years,[111] and if union participation continues to decline, even those unions that survive will be in a weaker bargaining position.[112]

IV. REASONABLE SOLUTIONS TO PREVENT EMPLOYER ABUSE

One solution would be for states to adopt a law similar to Wisconsin's, which prohibits an employer from implementing a mandatory microchipping program for its employees.[113] The Wisconsin Statute specifically provides that "(1) No person may require an individual to undergo the implanting of a microchip. (2) Any person who violates sub. (1) may be required to forfeit not more than $10,000. Each day of continued violation constitutes a separate offense."[114] Wisconsin is not the only state to pass a law that prohibits mandatory microchipping, but the number of states that have done so remains in the minority.[115] Laws that prohibit mandatory programs are a good first step, but the law needs to develop further to provide protections for the other issues that arise when an employer wishes to implement a microchipping program. While these laws protect an employee's privacy interest to an extent, they only do so in Wisconsin and the select few states that have also passed such a law. Further, these laws do not provide protection once an employee has volunteered to be microchipped.

---

110. Green, *supra* note 40, at 79.

111. Act 10 in Wisconsin, passed in 2011, stripped unions' ability to collectively bargain. Lydia DePillis, *Here's what happened to teachers after Wisconsin gutted its unions*, CNN (Nov. 17, 2017), http://money.cnn.com/2017/11/17/news/economy/wisconsin-act-10-teachers/index.html. It is likely that union participation rates will continue to decline as the result of the Supreme Court's ruling in *Janus v. AFSCME*, where compulsory union dues were held to violate the free speech rights of non-members. 138 S. Ct. 2448, 2460 (2018).

112. Even in the union context, there are those who argue there is still a disparity in the bargaining power between a union employee and an employer. Bagchi argues that the current statutory scheme is too weak, creating a false sense of union strength that does not actually exist. Aditi Bagchi, *The Myth of Equality in the Employment Relation*, 2009 MICH. ST. L. REV. 579, 580 (2009).

113. *See* WIS. STAT. § 146.25 (2006).

114. *Id.*

115. *E.g.*, N.D. CENT. CODE § 12.1-15-06 (2009); CAL. CIV. CODE § 52.7 (West 2009).

Another solution could be the adoption of the Restatement (Third) of Employment Law § 7.03,[116] which would make the analysis used in *Trotti* much simpler in the context of implanted microchips and other workplace technology that would have similar capabilities. Section 7.03 clearly states that an employee has a privacy interest against an employer's intrusion into specific things, including the employee's physical person.[117] Specifically, Restatement (Third) of Employment Law § 7.03(a) provides "[a]n employee has a protected privacy interest against employer intrusion into: (1) the employee's physical person, bodily functions, and personal possessions; and (2) physical and electronic locations, including employer-provided locations, as to which the employee has a reasonable expectation of privacy."[118] By making it clear that there is an expectation of privacy in the employee's physical person, there would not be a need for an analysis like that in *Trotti* as to whether the employee had an interest in the employer-provided locker.[119]

A violation of § 7.03 that meets the requirements of the Restatement (Third) of Employment Law § 7.06 may subject an employer to liability.[120] The requirements under § 7.06 are like those in *Trotti*; that "the intrusion would be highly offensive to a reasonable person under the circumstances."[121] Adopting sections 7.03 and 7.06 would act as a deterrent to employers that might otherwise abuse the capabilities of microchip technology programs implemented in the workplace.[122] This deterrent value is important given that implantable microchips already have the capability to measure the amount of sugar in one's blood and the potential for other types of tests measuring bodily functions that could be developed in the near future.[123]

---

116. Restatement (Third) of Employment Law § 7.03 (AM. LAW INST. 2013).

117. *Id.*

118. *Id.*

119. K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 637-38 (Tex. App. 1984).

120. Restatement (Third) of Employment Law § 7.03 (AM. LAW INST. 2013) (comment a).

121. Restatement (Third) of Employment Law § 7.06(a) (AM. LAW INST. 2013).

122. Currently, no states have adopted section 7.03 or section 7.06 according to the citing references on Westlaw. *See* Citing References to Restatement (Third) of Employment Law § 7.03, WESTLAW, https://1.next.westlaw.com/Search/Home.html?transitionType=Default&contextData=(sc.Default)&bhcp=1 (search Restatement (Third) of Employment Law § 7.03); Citing References to Restatement (Third) of Employment Law § 7.06(a), WESTLAW, https://1.next.westlaw.com/Search/Home.html?transitionType=Default&contextData=(sc.Default)&bhcp=1 (search Restatement (Third) of Employment Law § 7.06(a)).

123. *Glucose-Sensing RFID Microchip*, *supra* note 37.

Another solution would be to apply the tort of Unreasonable Publicity Given to the Other's Life.[124] Specifically, the Restatement provides that "[o]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[125] This restatement would provide for a remedy for type of violation to one's privacy not covered by the Restatement (Third) of Employment Law § 7.03; recovery for the heightened level of culpability exhibited by an employer that not only chooses to violate one's privacy, but then shares the improperly obtained information publicly.

The tort of Unreasonable Publicity has been discussed in the case law of nearly every state in the country.[126] The adoption of the Restatement (Third) of Employment Law § 7.03 would serve only to make it easier to support a claim under section 652D of the Second Restatement of Torts in those states that have adopted a version of this tort. Ideally, both restatements paired together would provide remedies to those employees that choose to get microchips embedded if an employer abuses its position and would serve as a deterrent to employers that choose to implement a microchip program.

In the context of public employees, there is also the option to extend the requirements of the Fourth Amendment and require a warrant for the government employer to use an embedded device to gather the information. Under the plurality approach in *O'Connor*, a warrantless search by a government employer is acceptable if certain conditions are met.[127] Specifically, a "search is reasonable if it is justified at its inception and if the measures adopted are reasonably related to the objectives of the search and not excessively intrusive [considering] the circumstances giving rise to the search."[128] This test, however, was in the context an employer-provided office space. In the context of an embedded microchip, it is

124. Restatement (Second) of Torts § 652D (AM. LAW INST. 1977)

125. *Id.*

126. Goodrich v. Waterbury Republican-Am., Inc., 448 A.2d 1317,1328 (Conn. 1982); Contrell v. Smith 788 S.E.2d 772, 786 (Ga. 2016); McCormick v. Okla. Publishing Co., 613 P.2d 737, 739 (1980).

127. City of Ontario v. Quon, 560 U.S. 746, 761 (2010) (applying the *O'Connor* plurality approach).

128. *Id.* (internal quotations omitted).

unclear whether the Court would even apply the *O'Connor* plurality approach because the microchip would be conducting a search of one's person. Public employees have the benefit of being able to secure meaningful protection from public employers through the Fourth Amendment because this would cross the line from searching an employer-provided space to a search of a person's body.

V. CONCLUSION

All employees currently enjoy some level of privacy protections in the workplace. These protections are important in a society that sometimes feels as if it is losing the battle to maintain a work-life balance. As technology further develops, the potential for it to be used to invade a person's privacy in ways never imagined can only grow. Embedded microchips have just begun to appear in the workplace, and it might be too soon to tell whether they will grow in popularity. Nevertheless, microchips serve to illustrate the increasing need to update privacy laws to reflect the unique considerations that technology introduces to this issue, particularly when the technology becomes a part of the person that cannot simply be turned off or left at home.

While foreign law does not provide any examples for potential laws,[129] there are some domestic laws that could prove to be useful if expanded or adopted to cover employment privacy interests. If all states adopt a law similar to that of Wisconsin to prohibit mandatory implementation, employees will have some leverage in denying a program, or coming to an alternative arrangement. Adoption of the Restatement (Third) of Employment Law § 7.03 would make the rights that an employee has in their physical person and bodily functions, among other things, more explicit, thus making it easier to inform employees of their rights and more likely that courts will rule in their favor. Finally, adopting and extending Restatement (Second) of Torts § 652D would give employees a separate cause of action if an employer makes information gained through an intrusion into seclusion known to the public, recognizing the additional damages caused by public disclosure.

---

129. For a discussion of European privacy rights in the workplace, see Lothar Determann et al., *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable In Europe, Destroyed In The United States*, 26 BERKELEY TECH. L.J. 979, 1018 (2011).