Chipping Away Employee Privacy: Legal Implications of RFID Microchip Implants for Employees

Article By
Mary Colleen Charlotte Fowler
University of Kansas School of Law

- Labor & Employment
- Communications, Media & Internet
- All Federal
- Missouri
- California
- Florida

Thursday, October 10, 2019

The Microchip

As society strives for greater production output, it embraces the brave new world of emerging technology. Enter the microchip, a radio frequency identification device (RFID), roughly the size of a grain of rice, used as a form of “tracking technology” for “property or employees.” The Food and Drug Administration (FDA) approved use of implantable microchips in humans for medical purposes, opening a Pandora’s box of rapid advancement and unsettled use of the technology.

Currently, the microchip is used as a means of access to medical records and financial transactions, a tool of convenience, and an instrument within the employment context to increase productivity and efficiency. With the swipe of your hand, you can unlock a door, purchase a snack, or log onto a computer system. The microchip’s appeal is tangible and embraced by an array of avant-gardists, from European partygoers to Wisconsin
workers, but with powerful technology comes potential for abuse. The ambiguity surrounding microchip technology leaves employees vulnerable. Although a relatively new technology, parallels with other forms of employee monitoring technology, such as GPS, provides rudimentary guidance to legal questions addressing employee microchips.

Since the FDA’s approval, human microchip implantation has unsettled many, especially after news reports revealed that CityWatcher, a Massachusetts company, had implanted microchips into two employees. Several states have responded by considering legislative steps to preemptively protect individual rights from the newly sanctioned technology, but only five states—California, Missouri, North Dakota, Oklahoma, and Wisconsin—have adopted statutes addressing human microchip implantation, with California and Missouri specifically addressing the employment context.

This tiny, but powerful technology is powered by RFID, which many industries use for tracking, screening, and efficiency purposes. There are four components to the microchip: RFID tags, RFID reader, antenna, and a database which stores memory to an external computer. An RFID tag is composed of a microchip and an antenna, which allows the implanted microchip to communicate a unique identification code to the RFID reader. The RFID reader contains an antenna, which “converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers.” The computer finally processes the data so the operator can make a decision, i.e. giving an individual access to a secured location.

The first component of an RFID microchip is the memory tag. RFID memory tags can either be passive or active. Passive tags derive power from RFID readers, transmitting radio waves for short distances. Active tags are battery-powered, making them more reliable for long distance communication and data storage with a data expansion function. This expansion function increases the technology’s capability, but its “greater transmission range presents a more substantial threat to data confidentiality and [an individual’s] privacy.”

Memory tags transmit data to RFID readers. Some tags can communicate with any reader, so the more ubiquitous readers become in society, the greater chance the tag will be scanned and data will be transmitted without individuals knowing. Memory tags are able to communicate with readers through the antenna.

The information the reader collects is stored in the database, including the “item identifier, description, manufacturer, the item’s movement, and location.” The database owners can connect the database to other networks, allowing sharing of data beyond the original database.

Microchip-generated data is vulnerable to hacking and potential misuse by employers. In 2006, Jonathan Westhues hacked and cloned an implantable microchip, disproving claims that the technology was “immune to theft.” Once cloned, the microchip copy functions like the original implant and can, for example, be used enter an employee's secured location. Without effective security measures, any compatible reader can read the memory tag data, allowing unauthorized readers can read or divert data communicated through the air.

Having discussed the components of RFID microchips, we now understand their potential uses and focus on the use of RFID technology in the form of implantable microchips in the workplace. Employers may find implantable microchips attractive because they afford a new
and more precise way to ensure worker productivity and security. For instance, employers may use microchip data to gather real-time computer or technological systems activity data, or make accurate calculations of tardiness, overtime hours, and workplace behaviors. These appealing features may pave the way for widespread microchip use in the workplace, placing employees in a vulnerable position with little protection and uncertainty regarding the courts’ response to legal questions arising from its use. An evaluation of the microchip’s impact upon employee autonomy and privacy requires us to examine the role of privacy and consent.

### Role of Privacy & Consent

*Griswold v. Connecticut* fostered the American idea that privacy is a “core aspect of individual liberty,” that deserves heightened protection within the law. It established the right to privacy as existing within penumbras of the Constitution. In particular, the Fourth Amendment has become a cornerstone of privacy law, specifically regarding individuals’ rights to be “secure in their persons... against unreasonable searches and seizures...” Privacy law is not only rooted in our American tradition but also the common law.

The common law protects four types of privacy interests: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) publicity placing a person in a false light, and (4) misappropriation of a person’s name or likeness. This Article focuses upon intrusion upon seclusion and its role in protecting employees’ privacy from microchip technology. The tort is available throughout the states as a claim against employers in the private sector. The tort involves an intentional intrusion, whether physical or non-physical, upon another’s private interests, which a reasonable person would find highly offensive. Employees have historically used this tort to challenge employer monitoring in the workplace.

Consent impacts privacy law. An individual’s consent effectively has transformative capabilities, such that “consent turns a trespass into a dinner party, a battery into a handshake, a theft into a gift, [and] an invasion of privacy into an intimate moment.” Consent’s role in the workplace is complex. Consent is an affirmative defense for employers against privacy torts, making it extremely difficult for an employee to bring a cause of action. The Restatement of Employment Law states that consent is invalid if “obtained as a condition of obtaining or retaining employment,” meaning that consent will not provide a defense to a privacy intrusion. However, this is not a general rule. It is up to states or courts to adopt this approach.

### Workplace Protections

**Common Law**: Though they are limited, employees have some privacy protection rooted in the common law. The effects of human microchip implantation could satisfy the elements of an intrusion upon seclusion tort. Microchip implantation is certainly an intentional and physical invasion into the body, and if unprivileged, would be categorized as a battery. It is not the physical implantation that would raise a possible intrusion upon seclusion claim. Instead, the tort would likely occur when an employer uses the microchip to excessively intrude upon an employee’s highly personal and sensitive data. For example, a reasonable person would find the microchip’s ability to detailly track his or her movement within the work environment highly offensive. Although this tort provides a potential cause of action for an employee against an employer, it is greatly weakened by the employer’s ability to easily eliminate an expectation of privacy by means of notice in a staff manual. Additionally, if an employee consents to microchip implantation, his consent would most likely be a
complete defense for the employer against any privacy claim.

**Constitutional Protections**: The Fourth Amendment protects public-sector workers.\[^{xlvi}\] In *United States v. Katz*, Justice Harlan, in his concurring opinion, created a reasonableness standard regarding the Fourth Amendment to determine whether a new technology is unconstitutional.\[^{xlvii}\] The test contains two parts: (1) the individual has a subjective privacy expectation, and (2) that the subjective privacy expectation in question is “one that society is prepared to recognize as ‘reasonable.’”\[^{xlviii}\] The Fourth Amendment’s application also extends beyond physical invasions to include technological invasions.\[^{xlix}\] Generally, it is only applicable in cases involving public sector employees, but courts apply a similar balancing test in the private sector where the “operational realities” of the employment context may decrease a reasonable expectation of privacy regarding private sector employees.\[^{l}\]

The Supreme Court, although unclear about what constitutes a reasonable expectation of privacy, has addressed Fourth Amendment implications of several new technologies, including GPS\[^{li}\] and real-time cell-site monitoring.\[^{lii}\] The Court has not addressed RFID technology, but because of the parallels between RFID technology and other technologies, such as GPS and real-time cell-site monitoring, the Fourth Amendment may be applied similarly. Historically, courts have found it difficult to define a reasonable expectation of privacy because an individual’s expectation of privacy is determined by his environment and his community standards.\[^{liii}\] This analysis is even more difficult in the employment context, because employers will issue equipment that has the capacity for private use (e.g. cell phones, laptops, etc.).

When determining a reasonable expectation of privacy, the Supreme Court recognized an employee may not have a reasonable expectation of privacy if an employer’s “noninvestigatory, work-related purpose” supersedes it.\[^{liv}\] The fact that equipment is employer-owned is not determinative of whether an employee has a right to privacy.\[^{lv}\] Instead, it must be considered in relation to the employee’s expectation of privacy in using that equipment.\[^{lvi}\] In *City of Ontario v. Quon*, a police officer used an employer-issued pager to send personal messages, for which the officer paid overage.\[^{lvii}\] The employer’s express, written policy was that there was “no expectation of privacy or confidentiality” regarding pagers and that employees would be subject to potential auditing and text messages would be treated similarly to e-mails.\[^{lviii}\] However, as officers began to pay overage fees, the Court found the employees developed an expectation of privacy regarding personal use.\[^{lix}\]

Implanted microchips, paid for by an employer, would likely qualify as employer-owned equipment, meaning an employee would have a reduced expectation of privacy regarding that particular equipment and could be subject to monitoring. Employer-issued implantable microchips are similar to the employer-issued pagers in *Quon*. The microchip, if employer-owned, could also serve personal uses because its function extends beyond workplace activities, such as holding medical information and access to financial data.\[^{lx}\] Because the data on the microchip is of such an invasive, personal nature, the employee may develop an expectation of privacy exceeding the privacy expectation outlined by the employer, the owner of the physical chip. Without clear guidance, these questions will most likely lead to litigation and further erosion of privacy rights.

**Limited Federal Protections**: The Electronic Communications Privacy Act (ECPA), enacted in 1986, regulates the monitoring of electronic communications.\[^{lxii}\] The ECPA prohibits interceptions or disclosures of any wire, oral, or electronic communications.\[^{lxiii}\] The Act is subject to a major exception—permitting employee surveillance “within the ordinary course
So, an employer could argue implantable microchips and their incidental monitoring is necessary for increased workplace productivity and also in the ordinary course of business, thereby avoiding the ECPA’s prohibition. Moreover, the ECPA has already fallen short in its application to modern monitoring technologies. Because ECPA application is questionable involving current technologies, it is even more uncertain whether the ECPA would apply to microchip communications, affording employees little protection against employers’ ordinary course of business argument.

**Analogous Technologies**

**GPS Surveillance Technology:** *Jones v. United States* established that individuals have a reasonable expectation of privacy regarding their long-term movements. In *Jones*, law enforcement obtained a search warrant to place a GPS tracking device on Jones’s vehicle and they proceeded to track his movements for twenty-eight days. The Government introduced this evidence at trial, but Jones argued it violated his Fourth Amendment rights and the Court agreed that the Government’s action constituted an unreasonable search under the Fourth Amendment. This reasoning should hold similarly in a non-criminal investigatory context, especially in a workplace environment where there is some expectation of privacy regarding an employee’s movements.

Microchip technology, unlike GPS, currently cannot track every individual movement unless it is paired to an external GPS source. Nonetheless, microchip technology can track an individual’s movements. Readers pick up RFID signals and send the information to external networks that catalogue the employee’s pattern of movement within the workplace. *Jones’* rationale that individuals have a reasonable expectation of privacy regarding long-term movements should extend to the microchip and employees in the workplace, even if restricted to defined space. Otherwise, employers may abuse this information, such as when they discover an employee’s workplace habits, ranging from bathroom breaks to determining which employees are meeting with each other, and then leverage this information against the employee by withholding wages, or worse, terminating them.

**Cell-site Location Information:** Cell phone signals continuously connect to cell-sites, owned by wireless carriers, creating precise, time-stamped records referred to as cell-site location information (CSLI). In *Carpenter v. United States*, the Court considered whether a person has a reasonable expectation of privacy regarding his cell-site location data and held that such information is protected by the Fourth Amendment, meaning the Government’s ability to obtain it is limited because of the data’s unique and historically-revealing nature.

The Court held the Government’s search of CSLI violated Carpenter’s reasonable expectation of privacy regarding his physical movements as pinpointed by CSLI. The Court reasoned that Carpenter had not given up his expectation of privacy under the third party doctrine. The third party doctrine, as established under *United States v. Miller* and *Smith v. Maryland*, asserts that a person does not have an expectation of privacy regarding information he voluntarily provides to a third party that is viewed in the ordinary course of business. The Court declined to extend *Miller* and *Smith* to include the collection of CSLI because of the unique and revealing nature of the data.

CSLI pinpoints an individual’s location based on cellphone signals. This also holds true for implantable microchip data, which workplace readers continuously collect and store either through passive tags in close contact with the reader, or through advanced active tags, allowing for continual data collection from longer distances. Also like CSLI, the
microchip data creates an historical account of an individual’s pattern of movements.\[lxxvi\] The Carpenter rationale should extend to microchips because employee microchip data is sent to an external database, allowing third parties to access data that creates a pattern of employees’ movements. Employers could abuse this by over-monitoring employees. For example, an employer could rely on location to pin a particular employee with a workplace violation or crime, shifting the presumption of innocence and placing a burden on an employee to prove or disprove his location. As pointed out in Carpenter, allowing access to this type of data subjects persons to “tailing” before they are even suspects, creating a surveillance environment that is counterintuitive to society’s view of privacy.\[lxxvii\]

**Legislative Action**

In response to privacy concerns about the microchip, several states have either proposed bills or enacted state legislation addressing forced microchipping of individuals.\[lxxviii\] Currently only five states have enacted state laws addressing this issue.\[lxxix\] Additionally, Florida’s bill, although unsuccessful in its passage, is worth including in our analysis. This Article highlights three of those states:

**California** In 2008, California created perhaps the most comprehensive law addressing implantable microchips. The statute states that “a person shall not require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device.”\[lxxxi\] The California implant definition covers implantable RFID microchip technology, but also leaves room for other forms of technology that could be similarly implemented.\[lxxxii\] The statute has a broad definition of person, which includes “an individual, business association, partnership, limited partnership, corporation...”\[lxxxiii\] The statute clearly extends to the private employment environment, addressing the various methods an employer could use to coerce an individual to implant a microchip:

‘ Require, coerce, or compel’ includes physical violence, threat, intimidation, retaliation, the conditioning of any private or public benefit or care on consent to implantation, including employment, promotion, or other employment benefit, or by any means that causes a reasonable person of ordinary susceptibilities to acquiesce to implantation when he or she otherwise would not.\[lxxxiv\]

**Missouri** primarily addressed the microchip and its relationship to the employment context, providing that “[n]o employer shall require an employee to have personal identification microchip technology implanted into an employee for any reason.”\[lxxxv\] “Personal identification microchip” encompasses implanted microchips and also covers devices that contain personal information or have a unique identifier that could be noninvasively transmitted or obtained.\[lxxxvi\]

**Florida:** Although the Florida bill proposal did not pass, it provides an extra element to include in any state’s future legislation addressing microchip implantation: informed consent. Florida proposed a bill to prohibit the implantation of microchips or similar monitoring devices in human beings.\[lxxxvii\] In particular, the bill focused on extending informed consent to implantable microchips or similar monitoring devices.\[lxxxviii\]

Though only a few statutes have been passed, the above States’ legislative responses to microchip implantation is helpful as other states begin to craft their own legislation in response to this new technology. Courts must address privacy rights in the private sector as they appear, and it is unclear whether state courts would follow the Restatement of Employment Law’s suggestions handling employee monitoring or employee privacy rights.
State legislatures could decide to follow the Restatement of Employment Law’s approach to employee privacy. The Restatement focuses on privacy rights of individuals currently in the work environment, while giving less weight to applicants.\[lxxxviii\] It defines privacy interests as “the privacy of the employee’s person (including aspects of his physical person []) as well as the privacy of the physical and electronic locations, including work locations provided by the employer, as to which the employee has a reasonable expectation of privacy.”\[lxxix\] The Restatement of Employment Law also suggests a cause of action for wrongful discharge when an employee is fired for refusing to allow an employer to invade a privacy interest.\[xc\] Additionally, the Restatement would hold employers liable for “third party access to such employee information with employee’s consent.”\[xci\] It is uncertain whether any particular state would incorporate these suggested principles, and states may not have a need to do so until an issue arises in court.

**Legislative Considerations**

Because of the novelty of implantable RFID devices, it is difficult to predict how conflicts between employers and their employees would be resolved. Moreover, it could take years before employers and employees know the answers to the multitude of legal questions implantable microchips may raise. This gap in the law presents an opportunity for legislatures to create certainty in the murky areas of privacy and employment.

While addressing employee privacy, the legislative response will depend upon the capabilities of the implantable microchip technology. Specifically, lawmakers should draft legislation addressing the two extremes of the microchip technology spectrum—passive tags with limited capabilities versus active tags with extended capabilities, which, in turn, would require different degrees of restrictions to protect employee privacy interests. When crafting legislation, states should consider the abovementioned state laws currently addressing microchip implantation and their most important elements: definitions, permitted technology, security, and consent.

**Definitions:** When crafting definitions, legislatures should make them broad enough to withstand technological advancements but narrow enough to foster technological innovation. For example, the definition of microchip should be similar to that of Wisconsin\[xcii\] and California,\[xciii\] which provides a broad interpretation of “microchip,” including unknown technology beyond RFID and any device used for identification and tracking. The legislative aim should be to make the law applicable to all persons in the relevant state or limit the law to the employment context, such as the Missouri law,\[xciv\] but encompass both private and public sector work environments, such as Oklahoma’s statute.\[xcv\]

**Permitted Technology:** States should also consider restricting the use of RFID technology in microchips. For example, instead of using standard RFID technology, such as current microchips use, the microchips could use a lesser form of RFID, such as near field communication (NFC) technology. NFC is used in pairing technology that requires extremely close contact for data transmissions.\[xcvi\] This could potentially curb the extent of the microchip’s tracking capabilities, thereby preserving some expectation of privacy for employees when they leave the workplace each day. However, NFC is still vulnerable to attacks and data modification and the technology should be explored in greater depth.\[xcvii\]

**Security:** State statutory guidelines can hold employers accountable to develop best practices regarding data security of employee microchips. States could impose heightened accountability upon employers if their employees’ microchip data is breached, misused by third-parties, or misused by employers themselves. Some requirements could include unique
reader systems for the employees’ microchips, encryption codes for over-the-air data transmission, and policies encouraging employees to take extra precaution when syncing personal information, such as medical or financial information, to their work microchip.

**Consent:** States should incorporate informed consent into their statutes, as Florida attempted in its bill. Potential microchip statutes should outline an employer’s disclosure obligations to his employees so that employees may give informed consent. When an employer is asking an employee to have a device surgically implanted in his hand, thereby eroding the employee’s reasonable expectation of privacy in the workplace and subjecting him to potential risks such as data breaches, the employer should have a duty to provide the employee with all the risks of such an implantation before the employee agrees.

In addition to informed consent, legislators should include provisions allowing for an individual to easily revoke consent, so employees could have it removed without fear of retaliation from their employer. Provisions should also establish ownership—employees should own the microchip, both the physical object and data collected on the microchip, once it is physically inserted into his person, even if the employer paid for implantation. Establishing ownership will prevent disputes when an employee is either terminated or leaves a company. It affirms an employee’s autonomy, reaffirming their power to choose implantation and serves as a reminder that the employee has the power to revoke their initial consent.

Legislatures should explore whether consent is even possible in this situation. Employers asking employees to implant microchips may become so standard that even if an employee has the opportunity to refuse implantation, it would still be to their detriment. One option to overcome this question of consent would be an outright ban of employment microchip use regardless of consent for employment-related purposes. No state has taken this approach. One benefit would be that the law would not fall behind the technology and would protect all classes of individuals, including employees. However, this statute would be a check on the individuality, independence, and availability of choice of all individuals, including employers and employees. The question becomes whether an employer’s legitimate business needs or whether an individual’s convenience preferences outweigh the state’s interest in maintaining and protecting employee privacy rights.

RFID microchip technology is here to stay. Because of its novelty, implantable microchip technology, although somewhat analogous to other forms of employee monitoring, presents a gap in the law. To create clarity where there is ambiguity, and to prevent future litigation, state legislatures should create laws protecting applicants, employees, and former employees alike from required or coerced implantation and removal of microchip technology. Technology is a convenient tool. We are not obligated to become slaves to our convenience, but instead can preemptively provide means of preserving the long-held American values of individual dignity and privacy.


authorities identify wandering Alzheimer’s patients, allow consumers to buy their groceries, literally, with the wave of a chipped hand.


[v] Herbert & Tuminaro, supra note 1, at 381.

[vi] Londberg, supra note 4.

[vii] Lewan, supra note 3.

[viii] Londberg, supra note 4.


[xii] Id. at 237–238.


Graveling, et al., supra note 13, at 7, 13.


Sade, supra note 17, at 1-2.

Id.

Id.


Id. at 22; Privacy Comm’r of Canada, supra note 17, at 28.

Hostetter, supra note 13.

GOA, supra note 21, at 2, 4, 9.

Id. at 9.

Id.


Ozer, supra note 29, at 112.

GOA, supra note 21, at 19.


See Griswold, 381 U.S. at 483–86.

U.S. Const. amend. IV.

[xxxvii] Victoria Schwartz, Overcoming the Public-Private Divide in Privacy Analogies*, * Title and Article in memory of Dan Markel who generously provided priceless written and verbal feedback including the suggestion for this title, and whose voice remains in my head whenever I am writing asking me, "Is this a Puzzle paper or a Problem paper?", 67 Hastings L.J. 143, 162 (2015–16).


[xli] Id. at 1008.

[xlii] See generally Willborn, supra note 40.

[xliii] Restatement (Second) of Torts § 892A(1) (1979); Restatement of the Law, Employment Law § 7.03 (noting “[c]onsent is also not effective if the employee is threatened with job loss for failing to consent.”).


[l] See also Ortega, 480 U.S. at 717 (plurality opinion; "The operational realities of the workplace . . . may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official.")


[li] Id. at 759 (referencing Brief for Electronic Frontier Foundation et al. 16–20, that a reasonable expectation of privacy by employees may exist since “many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency.”).
[i] Id.

[ii] Id. at 752.

[iii] Id.

[iv] Id. at 751.

[v] Lewan, supra note 3.

[vi] 18 U.S.C.S. § 2511; Wilborn, supra note 39, at 839–41; V. John Ella and Jackson Lewis, Employee Monitoring and Workplace Privacy Law, AMERICAN BAR ASSOCIATION Section of Labor and Employment Law National Symposium on Technology in Labor & Employment Law (Apr. 6, 2016) 8


[viii] 18 U.S.C.S. § 2510; Wilborn, supra note 39, at 841; Ella and Lewis, supra note 73, at 8.

[ix] Wilborn, supra note 39, at n.64.

[x] Jones, 565 U.S. at 430.

[xi] Id.

[xii] Id. 404–05.

[xiii] See Alisha D. Wright, Microchipping Employees: Do the Pros Outweigh the Cons?, Society For Human Resource Management (August 7, 2107) https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/microchipping-employees-do-the-pros-outweigh-the-cons.aspx (quoting Sarah J. Platt and Keith E. Kopplin noting that “depending on where access points are installed, an employer could gain useful information, such as how long an employee spent in the break room, in the same vicinity as another employee who was allegedly harassed, or where material went missing.”).


[xvi] Id. at 2217, 2218, 2220.

[xvii] Id. at 2214–20.

[xviii] Id. at 2216.

[xix] Id. at 2220, 2217.

[xx] Sade, supra note 17, at 1–2.

[xxi] Wright, supra note 68.


[lxxxii] Cal. Civ. Code § 52.7(h)(2)

[lxxxiii] § 52.7(h)(4).


[lxxxv] § 285.035(2).


[xci] Restatement of the Law, Employment Law § 7.05(b) (2015).


Copyright KU School of Law