CITY OF TOPEKA

GPS chipping your employees and other 4th amendment concerns

Amanda Stanley, City of Topeka
John Goodyear, League of Kansas Municipalities

THE LEAGUE OF KANSAS MUNICIPALITIES

Supporting Kansas Cities

www.lkm.org

GPS Chipping is not sci-fi

WVLT 8 KNOXVILLE. TN

News First Alert Weather Watch Live As Seen On WVLT Submit Photos & Video Making A Difference Spo

ADVERTISEMENT

Company to become first in U.S. to microchip employees

Image License
Photo: Three Square Market

TECHNOLOGY

Microchipping Employees: Do the Pros Outweigh the Cons?

By Aliah D. Wright
August 7, 2017

LIKE SAVE PRINT EMAIL REUSE PERMISSIONS



April 3, 2022
Volume XII, Number 93

THE NATIONAL LAW REVIEW

Advertisement

7 NEW ARTICLES

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

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."[i] The Food and Drug Administration (FDA) approved use of implantable microchips in humans for medical purposes,[ii] 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,[iii] a tool of convenience,[iv] and an instrument within the employment context to increase productivity and efficiency.[v] With the swipe of your hand, you can unlock a door, purchase a snack, or log onto a computer system.[vi] The microchip's appeal is tangible and embraced by an array of avant-gardists, from [vii] to [viii] but with

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

KU SCHOOL OF LAW The University of Kansas

Related Practices & Jurisdictions

Labor & Employment
Communications, Media & Internet

As technology evolves, how do we ensure compliance with the 4th Amendment?

| Overview of Today's Presentation

1 | 4th Amendment Test for a Workplace Search
2 | Section 1983 Cause of Action Test
3 | GPS tracking vehicles
4 | Cell Phones / IT / Public Record Laws
5 | Drug Testing and the 4th Amendment
6 | Biometrics

The 4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized

The 4th Amendment for Government Employers

Competing Rights at Stake for Employee Searches– Always the Case, but Different Equation for Government Actors

- Employers have the right to hire and fire, to discipline, monitor employee performance etc., but….
- Government employers owe more rights than private employers

The 4th Amendment for Government Employers

"Generally, government employers need neither a warrant nor probable cause to conduct a search that complies with the Fourth Amendment. Courts grant government employers wide latitude, requiring reasonableness under all the circumstances involved."

- Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 670 (1989)

O'Connor v. Ortega – Test Articulated

1. Did the employee have a reasonable expectation of privacy?
   - If no, 4th Amendment is not applicable

2. Was the search itself Reasonable?

1. Reasonable Expectation of Privacy

- Did the Employee have an Actual Expectation of Privacy?

- Was that Expectation Reasonable?
  - Workplace Definition in *O'Connor v. Ortega* helps to frame this
    - Is the item within the employers control? (Ex. Desks, Filing Cabinets, Computers)
    - Were employees put on notice that personal items may be searched? (*see United States v. Broadus*, 7 F.3d 460, (6th Cir. 1993); *United States v. Gonzalez*, 300 F.3d 1048 (9th Cir. 2002))

2. Reasonableness of Search

1. Was the Search Justified at its Inception?
    - Non-Investigative Work-related searches (ex. Finding a file)
    - Searches for Employee Misconduct (ex. Improper Computer Usage)

2. Was the Search Reasonable in Scope?
    - Reasonably related to the purpose of the search
    - Not excessively intrusive

Section 1983 Claim Requirements

1. Conduct of a person (person includes a municipality and municipal employees)
2. Action under color of state law
3. The action deprives a right protected by the US Constitution or federal law
4. Causation

GPS tracking Vehicles

Basic Question to 1st ask: Is GPS tracking a vehicle a search?

Answer: Yes per United States v. Jones, 565 U.S. 400, 132 S. Ct. 945, 946, 181 L. Ed. 2d 911 (2012).

Since it is a search, when can the government employer track a vehicle?

Cunningham v. New York State Dep't of Lab.,

Facts of the Case

- State of New York suspected employee of falsifying data
- Attached a GPS tracker to the employee's car
- Did not inform employee
- Monitored all movement for a month
- Employee Terminated for multiple employment violations including approving his secretary's timecard for hours worked while he was visiting her apartment

Court Held

- State action was a search
- Didn't need a warrant because it fell under workplace exception
- BUT search was unconstitutional under both state and federal constitution because it was unreasonable
  - Tracked employee on all evenings, weekends, and even on vacation
  - While he was not disciplined for conduct outside of business hours, because of the excessively unreasonable nature of the search, the Court required suppression of all the GPS data

Before deciding to implement a tracking program

1. Do you truly understand how the tracking technology works including what data it collects, where it sends data, and the parties that can see the collected data?
2. What privacy policies are you willing to implement to protect the data?
3. Have you ensured that your employee notifications regarding privacy accurately reflect the tracking technologies used?
4. Have you verified if any state or federal laws will affect your use of the technology?

Policy Best Practices for Tracking a City Vehicle

1. Notify employees they are subject to monitoring if they use city-issued vehicles or other property installed with GPS.
2. Inform employees they have no expectation of privacy as to their location and whereabouts when using city property installed with GPS.
3. Obtain the written consent of employees to be monitored by GPS on city-issued devices.
4. Verify the GPS surveillance programs comply with local legal requirements.
5. Limit the monitoring of employees to work time to avoid intruding on employees' personal lives outside of working hours.

Cell Phones / IT

- Unlike the private sector, employees **may** have a reasonable expectation of privacy in personal communications such as emails and text messaging.
- You can reduce that expectation through adoption of a policy that outlines areas subject to search
  - City Network
  - Files on Government Phone
  - Email

City of Ontario, CA v Jeff Quon 130 S.Ct. 2619 (2010)

Facts

- Police officer brought a §1983 action against city, police department, police chief, alleging that police department's review of officer's text messages violated Fourth Amendment, and asserted claim against wireless communications provider under Stored Communications Act (SCA).
- City issued pagers to its SWAT team with a monthly character limit
- After multiple months of overages, City did an audit to see if messages were work related

City's Search

- City's search was limited in scope.
- Only audited 2 months of texts
- Only looked at those sent while on duty
- Quon previously warned his messages were subject to search
- Found many Quon messages were not work related, and some were sexually explicit to both is wife and mistress; Quon had sent or received 456 messages during work hours in August of 2002 and no more than 57 were work related

Justice Kennedy held:

- Reversed the 9th Circuit
- The City's review of officer's text messages was reasonable, and thus did not violate Fourth Amendment.
- "The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

What to consider before a search

1. What is the legitimate justification for the search?
    1. Open Record Request (Non-investigatory)
    2. Work related misconduct (investigatory)
2. Does the employee have a reasonable expectation of privacy?
    1. Is it a personal or government phone? Does it matter?
3. Is the Scope of the Search Reasonable?
    1. Should your policy require more than person to sign off on a search as a "gut check" for reasonableness?
4. How does your Open Record Law Interact?

Finally, don't forget the Wiretap Act

The Wiretap Act allows an employer to intercept and use a communication when the interception is at least one of the following:

- Of a communication that is on the electronic communications system provided by the employer, when the interception is necessary to protect the rights or property of the employer (18 U.S.C. § 2511(2)(a)(i)).
- Consented to by at least one party to the communication (18 U.S.C. § 2511(2)(d)).
- Provided to a person authorized by law to intercept the communication, as defined in Section 101 of the Foreign Intelligence Surveillance Act of 1978 (18 U.S.C. § 2511(2)(a)(ii)).
- By way of an electronic communication system that is readily accessible to the public (18 U.S.C. § 2511(2)(g)).
- Made using "any telephone or telegraph instrument, equipment or facility, or any component thereof" furnished to the employer by a service provider in the ordinary course of its business and used by the employer in the ordinary course of its business (18 U.S.C. § 2510(5) (a)).

Employee Drug Testing

Drug Tests ARE Searches under the 4th Amendment

- *See Skinner v. Railway Labor Executives Association*, 489 U.S. 602 (1989)

Searches must then Be Reasonable

- Justified at the Inception
- Reasonable in Scope

So…When Can we Test?

1. Pre-Employment as a Condition for Employment – All Employees

2. Randomly – Safety Sensitive Positions

3. Upon Reasonable Suspicion – All Employees

What about Biometrics?

- Biometrics are "unique physical characteristics, such as fingerprints, that can be used for automated recognition."
- Local governments may be tempted to use biometrics for physical security and access to the worksite, to access technology devices, for covid screenings (temperature checks), and even attendance.
- Need to think about 4th Amendment but also other causes of action