International Municipal Lawyers Association

2022 Mid-Year Seminar, Washington DC

Section 1983

GPS chipping your employees and other 4th amendment concerns

April 8, 2022

Amanda Stanley, City Attorney for the City of Topeka, Kansas (author)

John Goodyear, General Counsel for the League of Kansas Municipalities

"©2022 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2022 Mid-Year Seminar, held April 8-11, 2022 in Washington, D.C. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents"

As a government employer, there are times I think we all shake our heads and wish we worked in the private sector. Things would be a lot easier if we didn't have to worry about pesky little things like the Constitution and how it interacts with §1983 claims. While this topic could be never ending dealing with several different constitutional amendments like the 1st amendment, 2nd amendment, 4th amendment, etc., today we are focusing on several different issues centering on the 4th amendment.

This presentation was actually inspired by a phone call I received about six years ago while working at the League of Kansas Municipalities from a city. I was asked if the city could GPS chip their employees in order to monitor their location during the work day. I flippantly answered without thinking that a Fitbit would be cheaper; however, the ability to easily track your employees has exploded over the last several years making this question something governmental employers should not treat flippantly. Where is the line? How does a government employer carefully walk the line of being a good employer and steward of the taxpayers' money and constitutional protections?

The 4th amendment to the constitution declares "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV

"When employers do search areas in which an employee has an expectation of privacy, courts do not apply the same analysis applied in the criminal context. 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).)" Constitutional Protections in Local Government Employment: Overview , Practical Law Practice Note Overview w-003-7117

> "In determining the appropriate standard for a search conducted by a public employer in areas in which an employee has a reasonable expectation of privacy, what is a reasonable search depends on the context within which the search takes place, and requires balancing the employee's legitimate expectation of privacy against the government's need for supervision, control, and the efficient operation of the workplace. Requiring an employer to obtain a warrant whenever the employer wishes to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unreasonable. Moreover, requiring a probable cause standard for searches of the type at issue here would impose intolerable burdens on

> public employers. Their intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this standard, both the inception and the scope of the intrusion must be reasonable." *O'Connor v. Ortega*, 480 U.S. 709, 710, 107 S. Ct. 1492, 1494, 94 L. Ed. 2d 714 (1987)

To sum this up in plain language, courts assess the legality of a workplace search as follows:

(1) Did the plaintiff have a reasonable expectation of privacy? Under this first prong, the court looks at:

-whether there was an actual (subjective) expectation of privacy; and
-whether the expectation was reasonable.

If the court finds there was no reasonable expectation of privacy, and therefore the Fourth Amendment does not apply, the plaintiff's case fails, and the test stops.

(2) If the court finds that the plaintiff did have a reasonable expectation of privacy, was the search was reasonable? Under this prong, the court looks at:

-whether the search was justified when it began; and
-whether the scope of the search reasonably related to the reason for the search and was not excessively intrusive.

To find for the government employee, the court must find that the employee had a reasonable expectation of privacy and that the search was not reasonable

Section 1983 creates a cause of action against any person depriving another of a federal constitutional or statutory right while using state government authority.

A Section 1983 claim requires:

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

(42 U.S.C. § 1983.)

This paper will examine the role of the 4th amendment in several different employment contexts.

1. GPS tracking cars

In *United States v. Jones*, the United States Supreme Court held that the Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. *United States v. Jones*, 565 U.S. 400, 132 S. Ct. 945, 946, 181 L. Ed. 2d 911 (2012).

In light of the fact that the attachment of a GPS device to a vehicle is a search, when can a government employer track a vehicle? In *Cunningham v. New York State Dep't of Lab*., 21 N.Y.3d 515, 518, 997 N.E.2d 468, 470 (2013), the State of New York, suspecting that one of its employees was submitting false time reports, attached a global positioning system (GPS) device to the employee's car. The employee was not informed of the GPS device and the devise monitored all of the car's movements for a month, including evenings, weekends and several days when the employee was on a vacation. Ultimately the employee was terminated for multiple employment violations including approving his secretary's timecard for hours worked while he was visiting her apartment. The court held that the State's action was a search within the meaning of the State and Federal Constitutions; however, that the search did not require a warrant as it fell under the workplace exception to the warrant requirement as recognized in *O'Connor v. Ortega*, 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987). Despite not requiring a warrant, ultimately the court still found the search did not comply with the state or federal constitution unless it was a reasonable search. In this case, the court held the search was unreasonable.

> "We cannot find, however, that this search was reasonable in its scope. It was, in the words of the *T.L.O.* Court quoted in *O'Connor,* "excessively intrusive." It examined much activity with which the State had no legitimate concern—i.e., it tracked petitioner on all evenings, on all weekends and on vacation. Perhaps it would be impossible, or unreasonably difficult, so to limit a GPS search of an employee's car as to eliminate all surveillance of private activity—especially when the employee chooses to go home in the middle of the day, and to conceal this from his employer. But surely it would have been possible to stop short of seven-day, 24–hour surveillance for a full month. The State managed to remove a GPS device from petitioner's car three times when it suited the State's convenience to do so—twice to replace it with a new device, and a third time after the surveillance ended. Why could it not also have removed the device when, for example, petitioner was about to start his annual vacation?
>
> It is true that none of the evidence used against petitioner in this case resulted from surveillance outside of business hours. Ordinarily, when a search has exceeded its permissible scope, the suppression of items found

> during the permissible portion of the search is not required (*see United States v. Martell,* 654 F.2d 1356, 1361 [9th Cir.1981] [excessive length of detention did not taint search where nothing new was learned "during the unlawful portion" of the detention]; *United States v. Clark,* 891 F.2d 501, 505 [4th Cir.1989] [same]). 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" (*Weaver,* 12 N.Y.3d at 441, 882 N.Y.S.2d 357, 909 N.E.2d 1195). 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 the GPS evidence here; the State has disclaimed any reliance on the balancing test that we use when deciding whether to invoke the suppression remedy in administrative proceedings (*see Matter of Boyd v. Constantine,* 81 N.Y.2d 189, 597 N.Y.S.2d 605, 613 N.E.2d 511 [1993])." *Cunningham v. New York State Dep't of Lab.,* 21 N.Y.3d 515, 522–23, 997 N.E.2d 468, 472 (2013)

If a City is going to GPS track its vehicles, here are some common things that should be considered / performed:

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.

See Privacy in the Employment Relationship, Practical Law Practice Note 6-517-3422 for more helpful tips.

Local Governments can learn valuable lessons from best practices used by companies deploying tracking technologies. Before utilizing GPS tracking, think through the following:

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?

For more information on best practices, check out: Tracking Technologies: Privacy and Data Security Issues, Practical Law Practice Note w-006-5583

2. Cell Phones / IT

Employees may have a reasonable expectation of privacy in personal communications such as emails and text messaging. An employer can reduce that expectation of privacy through the adoption of a policy outlining the areas subject to search such as files on the city's network, files on a government phone, etc. Before beginning a search, make sure there is a legitimate justification for the search such as a non-investigatory work-related purpose (need to find a file to respond to an open records request) or a legitimate investigation of work-related misconduct. Make sure to evaluate the reasonableness of the scope of the search. In the City of Topeka, both the Human Resources Director and the City Attorney must sign off on the search of an employee's files.

There is no blanket caselaw rule drawing a distinction between an employer owned device and a personal device. Follow the analysis. What matters is the reasonable expectation of privacy.

When crafting a good policy for employee use of government-provided email systems and phones, include statements that the employee has no expectation of privacy and that files may be searched in response to open records requests or in response to litigation. It is important to outline limits on personal use of government equipment and email at the beginning and be clear on what the city's policies are for encryption and password protections.

Wiretap law Exceptions?

"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)). This exception commonly applies to a telephone service provider's inadvertent interception of a telephone conversation during the provider's routine maintenance. More recently, the exception has been analyzed in the context of email or internet service providers that capture data about their account holders for marketing and advertising purposes. Some judges have adopted a narrow view of the exception (see, for example, Kirch v. Embarq Mgmt. Co., 702 F.3d 1245, 1251 (10th Cir. 2012), Hall v. Earthlink Network, Inc., 396 F.3d 500, 504-05 (2d Cir. 2005), and In re Google, Inc., 2013 WL 5423918, at *8 (N.D. Cal. Sept. 26, 2013)). Other judges have taken a broader approach (see In re Google Privacy Policy Litig., 2013 WL 6248499, at *10-11 (N.D. Cal. Dec. 3, 2013))."

Electronic Workplace Monitoring and Surveillance, Practical Law Practice Note 1-506-8862

What about Public Record Laws?

In Kansas, a local government is required to provide records regardless of the location they are stored. It is extremely important that personnel policies are clear that an employee must cooperate with an open record request. Policies should include requirements that any work done on a personal email or phone be forwarded to a government account, statements that substantive work should not be done on a personal account, and a statement that the employee understands and agrees to comply with the Open Records law. It is essential that you understand your state's record laws BEFORE a request.

3. Drug Testing and the 4th Amendment

See attached article

3. Biometrics

What are biometrics? According to Homeland Security, biometrics are "unique physical characteristics, such as fingerprints, that can be used for automated recognition." The use of biometrics is greatly expanding. Just think about how far cell phones have come in the past ten years. First it was a fingerprint, and now, even your face that can unlock a screen. 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.

In addition to possible 4th amendment concerns, there are multiple cause of actions that can result from use of biometrics as an employer. These include Genetic Information Nondiscrimination Act (GINA), Religious discrimination,

Age discrimination, Stored Communications Act, Electronic Communications Privacy, and State law claims, including unlawful acquisition or retention of biometric identifiers or improper destruction. Think through the new implantation of biometrics methodically to ensure liability is minimized.