



Best Privacy Practices For Employer-Issued Fitness Trackers

Insights

5.01.19

Workplace technology has been ever-changing in the past few decades: from desktop computers, to mobile phones, to laptop computers, to smartphones. Now, smart watches are capable of receiving text messages and phone calls, tracking sleep, tracking daily fitness activity and more (cue “Black Mirror” montage). What does it mean for employees’ privacy when the technology is advancing at such an astronomical rate?

The Extent Of An Employee’s “Right To Privacy”

An employee’s right to privacy largely depends on where and how the employer is accessing personal information. For instance, most employees believe their online social media accounts (whether set to “public” or not) are private; that their employers should not view their accounts (even if the employee is “trolling” the company); and that employment decisions should not be made based on online comments.

However, as we know now, employees cannot expect such privacy, particularly when employees access their social media accounts on work-issued devices (e.g., laptops or smartphones). Similarly, employees may expect a right of privacy when it comes to their personal email accounts, but for the same reason, if accessed on a work-issued device, that right of privacy dwindles.

In fact, employers often require employees to provide them access to accounts or services the employer provides. Even where states have stepped in to regulate employee use of online accounts, employers’ rights generally are respected when the employer owns or subsidizes the device. For example, [the Wisconsin Social Media Protection Act](#) restricts employer actions that interfere with employees’ online activities, but it does not prevent employers from requiring that their employees provide access to information on an electronic device (e.g., computer or cell phone) supplied or paid for by the employer.

But what happens when employees’ health data collides with devices provided by the employer?

Technology And Healthy Living In The Workplace

Many employers have committed to promoting healthy living by implementing health and wellness programs, ranging from smoking cessation programs to “biggest loser” weight loss challenges. The goal is to help employees stay fit and healthy, because healthy employees tend both to be more productive and to incur fewer health care costs. According to the National Council on Strength & Fitness, employers save an average of \$4 for every \$1 spent on employee wellness.

fitness, employers save an average of \$0.10 for every \$1 spent on employee wellness.

Recently, employers also have begun providing employees with fitness trackers, such as watches and phone application subscriptions, and encouraging them to voluntarily sign up for digital health monitoring. Employers also may request that employees complete a biometric health screening that identifies certain health goals.

Typically, employees are promised cash, reduced premiums or reimbursements for co-payments and deductibles, which have increased significantly as health care costs continue to rise. Fitness trackers are steeply discounted or even handed out free if the employees sign up for an employer-sponsored health and wellness program. According to the Kaiser Family Foundation's [annual survey](#), 21 percent of employers that offer health insurance collected data from wearable devices last year, up from 14 percent in 2017.

This compilation of employee data is part of a concerted effort to improve the health of an employer's workforce. As a result, employers have access to the information transmitted from the fitness trackers. Depending on the device's sophistication, the employer can see how many steps the employee takes, the distance walked, the hours the employee spends in a sedentary state, 24/7 heart rate, and sleep duration and quality. If an employee is too sedentary, some fitness trackers will alert the employee to get moving. Or, depending upon the setup of the fitness tracker, the reminder or check-in call can come directly from the boss.

One brand, in particular, has developed a program especially for its corporate clients. Fitbit has designed an activity and sleep tracker (called Fitbit Inspire) for the company's "corporate, wellness, health plan and health systems partners and customers of their organizations, participants and members" (i.e., if you are not employed by or a member of one of these organizations, you will not be able to obtain one of these trackers). Fitbit added a call service that will reach out to individual workers, via text messages and phone calls, when the employee's data shows they are falling short of fitness goals.

Concerns With Data Collection

Opponents of the employer-provided fitness tracker trend believe employers will inappropriately utilize the information retrieved from the fitness tracker. Organizations concerned with employee privacy suspect the use of fitness trackers and the information generated from fitness trackers will cause employers to favor healthier employees over others. Questions are being asked about how much data the tracker can obtain and share with employers.

Will employers be able to tell who smokes? Who uses the bathroom most and may be pregnant or have prostate trouble? Who visits the vending machine or kitchen the most? Many fitness trackers have GPS capability, and some employers use GPS to track employees' movements while working, but will employers begin tracking what employees do on the weekends or in their free time? Will employers be able to track drug use via these devices? If employers are accessing this data, are they studying it and making decisions based on the information? Additionally, many opponents believe that employees do not really have a "choice" in opting into their employer's health and wellness

programs.

While the employer-provided fitness tracker trend is growing at a significant rate, it is unlikely the law will advance as rapidly. However, there is current legislation that can affect what an employer can do with information obtained by fitness trackers, and there are best practices that employers can implement to mitigate risk.

While the U.S. Supreme Court already has suggested that employees may lack any reasonable expectation of privacy in employer-provided technological equipment, some states have passed legislation regarding limitations surrounding employees' privacy. In fact, some states have passed legislation limiting what employers can do with employees' biometric data (e.g., [the Illinois Biometric Information Privacy Act](#)).

Employer Best Practices

While there are some legal risks involved in outfitting your workforce with fitness trackers, and the law is not fully developed, there are ways to mitigate these risks.

You should not require employees to use fitness trackers or fine employees who opt out of the program. You should obtain written consent from employees who wish to enroll in the program before they are issued fitness trackers. You should also implement a policy relating to the proper use of information obtained from fitness trackers. The policy should describe the reason the company implemented the program, the nature of the tracking device, the data being tracked, how you will use (and not use) the data, and how you will keep the data secure. Notice to the employee is key when establishing what privacy employees can reasonably expect.

Additionally, in this age of data breaches, the more data fitness trackers record, the greater the risk the information will be compromised. Privacy risks are relatively low for fitness trackers that collect nondescript data such as activity, steps, and calories. You should consider providing fitness trackers that only track basic, relevant fitness information. Additionally, you should limit the nucleus of individuals who may review the data and ensure that the information technology department has implemented data security protocols that protect this information just as rigorously as you protect trade secret data.

You also should consider obtaining fitness tracker information through a service that limits how you will receive the information. For example, Fitbit's privacy agreement aims to prevent employers from accessing information employees have not agreed to share; instead of sending specific results regarding individual employees, employer program administrators receive reports in aggregate form. If you cannot determine exactly whose fitness information you are reviewing at any given time, you can mitigate risk of privacy or discrimination complaints based on information obtained from fitness trackers.

Bottom Line

Employers that have implemented or are interested in implementing health and wellness programs that include providing fitness trackers to employees should remain concerned and committed to protecting employees' personal and health information and should refrain from inappropriately

protecting employees' personal and health information and should refrain from inappropriately using employee data obtained by fitness trackers. You should work hand in hand with your employment counsel to ensure you are addressing all of these concerns and complying with local laws.

For more information, contact the author at LHebert@fisherphillips.com or 713.292.5603. A version of this article originally appeared in [Law360.com](https://www.law360.com).

Related People



Lariza Pruneda Hebert
Of Counsel
713.292.5603
Email

Service Focus

Privacy and Cyber

Counseling and Advice