Client Alert: Macro-Level Issues to Consider When Microchipping Employees

Related Attorneys

Jackie Ford

Michael C. Griffaton

Related Services

Data Strategy, Privacy and Security

Labor and Employment

CLIENT ALERT | 8.10.2017

"Big Brother is watching." ~ 1984, *George Orwell*

For years, pet owners have implanted RFID (radio frequency identification) microchips in their dogs and cats to help track the animals if they get lost. Now, some business owners are giving employees the option to have themselves microchipped as well. Before rushing to embrace RFID technology in this fashion, employers should consider potential legal ramifications.

RFID Technology

There are two types of RFID devices – passive and active. A passive RFID chip lacks an internal power source like a battery, so it activates from the signal that is sent by the scanner that reads it, usually in close proximity. A passive RFID chip cannot send signals about location-based data. By contrast, an active RFID has a power source that enables it to transmit a signal continuously or on command.

Both forms of RFIDs are ubiquitous, being used for everything from logistics to tracking inventory, to race timing and conference attendee tracking, to materials management and access control. In August 2017, a Wisconsin company (Three Square Market) offered its employees the opportunity to have a microchip inserted into their hand allowing them to log into their computers, open doors, and buy snacks from vending machines by waving their hands. According to the company: "There is no GPS tracking. We can't track when you go to the restroom, we can't track when and where you are coming and going – it's purely for convenience." A Swedish company called Biohax International also has been selling RFID chips and implanting them in willing individuals. In fact, the Swedish national rail company has started scanning passengers' hands as many have had RFIDs implanted in them in lieu of using paper tickets. These uses of RFID chips raise questions about what is stored on the chip, how the chip is used, and who can access the information – which will only multiply as RFID technology evolves.

Potential Issues for Employers

The Wisconsin company made headlines with its "voluntary" employee microchipping. But can employers require RFID-implantation as a condition of employment? Ironically, in 2005, Wisconsin became the first state to enact legislation that prohibits implanting RFID microchips into people without their consent. California, North Dakota and Oklahoma also prohibit the mandatory implantation of RFID chips, and in February 2017, similar legislation was introduced in Nevada.

Mandatory microchipping implicates issues of religious accommodation. The Fourth Circuit Court of Appeals recently found an employer had discriminated against an employee by requiring him to use a biometric hand scanner. The employee said that doing so would compromise his religious beliefs regarding the Biblical concept of the "Mark of the Beast" (even though it wouldn't leave any mark) and sought a religious accommodation, which the employer refused. Employees may raise similar complaints against mandatory RFID implanting.

While Three Square Market claims its RFID chips cannot directly track employees' movements, RFID chips can certainly reveal where and when an employee accessed an RFID-enabled computer, door or vending machine. That same chip could later be used to track the length of employee breaks or the person's location. While RFID chips can only be tracked when in close proximity to readers, the proliferation of readers could make tracking easier. And as technology evolves, distance may have less of a restriction. Additionally, companies may decide to use RFID chips that are active and provide GPS data on employee whereabouts. Aside from basic privacy concerns, tracking employees could run afoul of state laws that prohibit employers from taking adverse action against employees who engage in lawful off-duty activities (like risky hobbies).

What is stored on the RFID also raises privacy concerns. Can the chips monitor employee health and wellness? If the chip contains employee health information, the employer may gain access to health information revealing an employee's genetic condition or disability – implicating the federal Genetic Information Nondiscrimination Act, the Americans with Disabilities Act, and similar state laws.

Any computer technology is vulnerable to hacking. Implanted RFID chips could be vulnerable to cyber attacks in which information on the chip is replicated, corrupted, modified or copied – resulting in identity theft.

Finally, what happens when the chipped employee leaves? Can he or she remove the chip? What happens to the data stored on it?

Conclusion

The Wisconsin company's CEO sees "the use of RFID technology to drive everything from making purchases in our office break room market, opening doors, use of copy machines, logging into our office computers, unlocking phones, sharing business cards, storing medical/health information, and used as payment at other RFID terminals. Eventually, this technology will become standardized allowing you to use this as your passport, public transit, all purchasing opportunities." Employers need to weigh these "benefits" against the privacy and other legal considerations that govern the workplace. If you have questions about issues related to RFID in the workplace, contact your Vorys lawyer.