MARCH 7, 2007 / ISSUE NO. 650

CCH
Human Resources Management
Ideas & Trends
A CCH PUBLICATION

EMPLOYEE RELATIONS

States regulate use of microchips as tracking device

A Georgia legislative committee recommended in February that the state ban employers from implanting microchips in their workers' arms to track their whereabouts, according to the Atlanta Journal-Constitution. You'd think it might go without saying that such conduct would be a no-no for employers. Yet Georgia is not the first state seeking to get in front of the issue, fearing potential abuse of the rapidly emerging technology.

States attempt to get ahead of the issue

Georgia's House Study Committee on Biological Privacy, which was created to look at ways to protect "biometric" information, issued the recommendation to ban implanting microchips on February 6, along with its findings. The microchip ban is one of several actions proposed in the individual privacy realm, but this threat seems the most ominous. However, "[the legislative proposal] is not a provocative thing we cooked up," said State Rep. Ed Setzler (R), who chairs the committee, as quoted in the AJC. "It actually has been done in another state."

Indeed it has. Last May, Wisconsin Governor Jim Doyle signed 2005 Wisconsin Act 482 into law. The statute prohibits the required implanting of microchips in humans, and violations carry a $10,000 fine per day. While that state's Legislative Reference Bureau noted it was the "first law of its kind in the nation," at least 17 additional states are considering such measures, including Michigan, Oklahoma and North Dakota. A pending New Jersey bill provides that individuals could not be coerced into being implanted with such devices, would require written informed consent before implantation, and would require that those implanted with chips could remove the devices at any time.

According to Dale L. Deitchler, shareholder in the Minneapolis office of Littler Mendelson, P.C., Florida legislators have also addressed the issue, proposing standards applicable for bail bond employees relating to Radio Frequency Identification Devices (RFID). He says, however, that the legislation is designed more from a technical/security perspective than as employee protection legislation. The Florida legislation has not passed.

Deitchler also pointed out Rhode Island legislation, proposed in 2005, that would have restricted RFIDs for public employees, and, according to Deitchler, in late 2006 New York legislators proposed an RFID

continued on next page

TECHNOLOGY

HR has difficult job of balancing all generations in workplace, from "You-Tubers" to the Atari generation

HR most definitely can accommodate the various generations representing today's workforce, but realistically speaking, it won't be easy. The world of work is rapidly changing. You see it every day in the workplace, where long-standing business protocols are quickly being radically altered by technology and virtual offices.

"Between user generated content and consumer oriented gadgets and gizmos, the technology train is way out of the station and HR can only try to keep up," said Richard Moran, Ph.D., a partner at the venture capital firm Venrock Associates. As each new generation brings 'their' tech into the organization it will only create more issues and opportunities to deal with. For example, the current buzz for the incoming college class is all about 'YouTube.' What will the Company do if someone secretly videos a manager giving a talk—particularly a bad one—and it shows up on YouTube? Is privacy

continued on page 36

INSIDE

Wolters Kluwer
Law & Business

MICROCHIPS

continued from front page

task force that would evaluate, among other things, use of RFIDs by employers. "At the federal level, a senate bill was introduced in July 2006 that would have banned involuntary implantation of microchips by private companies or the government," said Deitchler, who continued, "none of this legislation has passed."

In January, Colorado State Rep Mary Hodge introduced House Bill 1082, which would make it a misdemeanor in the state to "microchip" people to track workers' movements or for other unsavory purposes, the Rocky Mountain News reported. The measure has since been put on hold for further research—and after considerable ridicule in the statehouse.

"Of course employers interested in microchipping employees in all states need to be concerned with a whole range of issues relating to the common law of privacy (and diminishing or extinguishing expectations of privacy), occupational safety and health concerns and labor law bargaining requirements, to name just a few," said Deitchler.

Microchipping employees may not be least intrusive means

Is this a solution without a problem? Is the ridicule justified? After all, microchips—"RFIDs," or radio frequency identification devices, which the FDA cleared for human use for medical purposes in 2004—are already used to ensure "wander prevention" of long-term care residents, to protect infants in hospital maternity wards, even to locate missing pets. Some healthcare practitioners praise the use of such devices as a revolutionary and potentially life-saving means of quickly accessing patient health information.

The information emitted from a microchip is a mere number or code which is recognizable by the receiving database, but has no meaning without being cross-referenced against information in that database. Therefore, the information emitted by an RFID chip would not be usable to someone who intercepted that information. On the other hand, the slippery slope is here in sharp relief. Columbian President Alvaro Uribe suggested Columbian seasonal workers should have microchips implanted before being allowed to enter the United States, according to U.S. Senator Arlen Specter (R-Pa). Such a proposal begs the question: does this seem benign?

"When microchipping becomes common in the general public, when there are ways to assure employees that it is not being misused to track non-work activities, when the convenience is perceived as more beneficial than the intrusiveness for all involved, then you might see more widespread use."

What about employee privacy? "My initial reaction to the implanting of employees with microchips is that this is not something you're likely to see widespread use of for some time," said Deitchler. "There has already been pushback by employee privacy advocates with employers using employee monitoring and data storage devices employing GPS and radio frequency identification tags, and that reaction has come without the added issue of the invasive aspect of embedding a chip into the skin. Alternative methods to accomplish the same goals (primarily access) for the foreseeable future such as standard security cards, even biometric methods such as fingerprint and retina scans, will continue to be preferred by the vast majority of employers," Deitchler continued.

Not all employers are seeking alternatives to microchipping their employees and instead are turning to organizations like VeriChip Corporation, one of the most prominent device makers. VeriChip claims its RFID systems are installed in over 4,000 locations in healthcare, security, government and industrial markets. The technology promises a host of other potential conveniences—like unlocking a car with the wave of one's hand. And there are anecdotal reports that some employers have already implanted microchips in employees anyway, to be used as electronic keys and for other security-related purposes.

"Embedding chips raises privacy/intrusiveness concerns both physically and with respect to the scope of the capabilities it yields to employers," said Deitchler. "Specifically, the primary use for imbedded microchips at this stage is access and entry in high risk security environments, but there are less intrusive ways to accomplish the same goal, such as fingerprint or retina scans or even RFID badges or smart cards, such as those developed by the Department of Homeland Security."

Deitchler continued, "these alternative methods are not just physically less intrusive, they also do not carry with them the perception that employers are monitoring employees' every move—chip vendors indicate they are not equipped for tracking, but the literature on RFIDs generally indicates tracking capability. While the chips have been described as smaller than a grain of rice or even about the size of a grain of sand, embedding them is invasive, and there are broad-based privacy concerns with the limits of what the chips will be able to reveal to an employer and what an employer is entitled to know."

continued on next page

Human Resources Management Ideas & Trends

Managing Editor
Heidi J. Henson, J.D.

Contributing Editors
Lisa Milam-Perez
Joy Waltemath

HUMAN RESOURCES MANAGEMENT—Ideas & Trends (USPS 680-810)(ISSN 0745-0613), a CCH editorial staff publication, is published semi-monthly (twice a month) by CCH, a Wolters Kluwer Business, 4025 W. Peterson Ave., Chicago, Illinois 60646. Periodicals postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO HUMAN RESOURCES MANAGEMENT—IDEAS & TRENDS, 4025 W. PETERSON AVE., CHICAGO, IL 60646. Printed in U.S.A.

MICROCHIPS

continued from previous page

Employers justify microchipping by citing advantages

Employers who track employees with RFIDs justify implanting their employees with an electronic device by pointing to the multiple advantages such devices can potentially offer. RFIDs, for example, can enhance security, create a more seamless way to enter and exit a workplace, aide in the investigation of incidents or employee misconduct, and account for employees during workplace emergencies. Additionally, RFIDs can assist in the implementation of evacuation plans, limit access to confidential business information or medically sensitive storerooms and, when linked to employee medical records, it can assist in the care of an injured worker.

Microchips can also add an additional level of protection in high-risk industries. "Embedding them would resolve issues pertaining to loss of, for example, a badge or security card," said Deitchler. "In the extreme, though, in safety-sensitive positions, chip embedding could increase the safety risk to an employee targeted by virtue of the chip, and unseemly characters who would stop at nothing to get the chip—cutting it out, amputation, even murder."

This will definitely require a policy. An organization that decides to implant RFIDs in its employees will absolutely and without question need to create a policy before doing so. Even before the policy is created, however, other issues should be raised. "There is no question that in a unionized environment, for example, microchipping employees could not occur without first raising and bargaining over the issue," said Deitchler. "Additionally, all employers should provide as much advance notice as possible, laying out the business rationale, explaining in detail the capabilities of the chip to be implanted, the method of implantation, risks associated with implantation and processes and risks associated with chip removal."

When you get down to creating a policy, "notices communicating microchipping policies to employees should include a clear disclaimer indicating that the technology is in a rudimentary state, that long-term studies have not been conducted concerning the medical implications of imbedding chips and impose reporting requirements if complications arise," suggested Deitchler. "Acknowledgement of receipt of notice and that participation is voluntary, and where lawful, a release of claims should be secured."

"Of course employers interested in microchipping employees in all states need to be concerned with a whole range of issues relating to the common law of privacy, occupational safety and health concerns and labor law bargaining requirements, to name just a few," said Deitchler.

Deitchler also suggested that written policies should address how long data is stored, and that a corporate compliance/oversight officer should be appointed to monitor both the program and information generated through the program. "Medical and legal counsel should, of course, be consulted in preparing notices, policies and releases, if any," said Deitchler.

Looking toward the future

"This is a technology that may gain acceptance long term," said Deitchler. "In fact, it may ultimately be desired by employees as it gains broader acceptance within society in assisting healthcare professionals in providing particularly emergency medical treatment."

Deitchler reminded us that drivers' licenses and social security numbers were new at one point, as were vaccinations. "From a medical perspective, there is already more widespread use than in the employment environment," he said. "When microchipping becomes common in the general public, when there are ways to assure employees that it is not being misused to track non-work activities, when the convenience is perceived as more beneficial than the intrusiveness for all involved, then you might see more widespread use."

That said, however, Deitchler pointed to a number of unresolved technological issues, including an employee's ability to ensure that tracking is limited; what to do if an employer changes their security system or the chip becomes outdated; and what to do if an employee changes jobs. Additionally, some of the public information indicates chips can be "skimmed and cloned" extinguishing the security value of using them.

"Again, when there is more widespread use in the general public, likely for healthcare reasons, and the answers to some of the technology questions are more defined, then you may be seeing more employers interested in this kind of technology, but that is likely years away," concluded Deitchler.

Workplace security is often cited as a benefit organizations may enjoy through employee microchipping. Quite often, workplace security policies must take into consideration an employee's right to privacy. For a discussion of how to balance employee privacy with workplace security, check out the HR Practices Guide ¶4261 through ¶4262E. ❑

ON-LINE HR POLL

Are surveillance cameras in use by your employer?

Yes, employees are aware of & approve of their use..... 36%
Yes, employees are aware of & disapprove of their use 7%
Yes, but employees are not aware of their use 7%
No, we do not use surveillance cameras 50%

Results from 2/1/2007 through 2/23/2007; 223 respondents.

To participate in the latest online HR Poll, visit http://hr.cch.com today.