Do Employee Chip Programs Cross Privacy Boundaries?

Three Square Market, a Wisconsin-based software developer for vending machines, recently offered a voluntary program where employees could elect to have a microchip implanted in their hands in order to facilitate common office functions. While this program was entirely voluntary, more than fifty of the company's eighty employees agreed to take part. Each of these employees was injected with a Radio-Frequency Identification (RFIC) microchip in his or her hand with the goal of making their lives at the office easier.

The chip allows Three Square employees to navigate the office without the aid of a company badge or other device: unlocking doors, linking credit and debit accounts for purchase with the wave of a hand, logging into computers, and storing personal information. With more than half of Three Square Market employees participating in this program, it is clear employees are interested in making these types of workplace actions as simple as possible. However, no matter how easy these microchips might make office tasks, implanting chips in employees raises significant ethical and privacy issues.

The chips do not track the location of employees, as there is no GPS capability programmed into these chips; but what if such tracking capabilities are enabled in the future? Although the program is voluntary, are there potential privacy boundaries being violated? And what is the potential that a chip containing the personal data of Three Square employees including their credit and debit cards, could be hacked?

While Three Square Market has taken the position that the program is legally compliant, there is sure to be a heated debate over the ethics of these kinds of employee microchip programs.