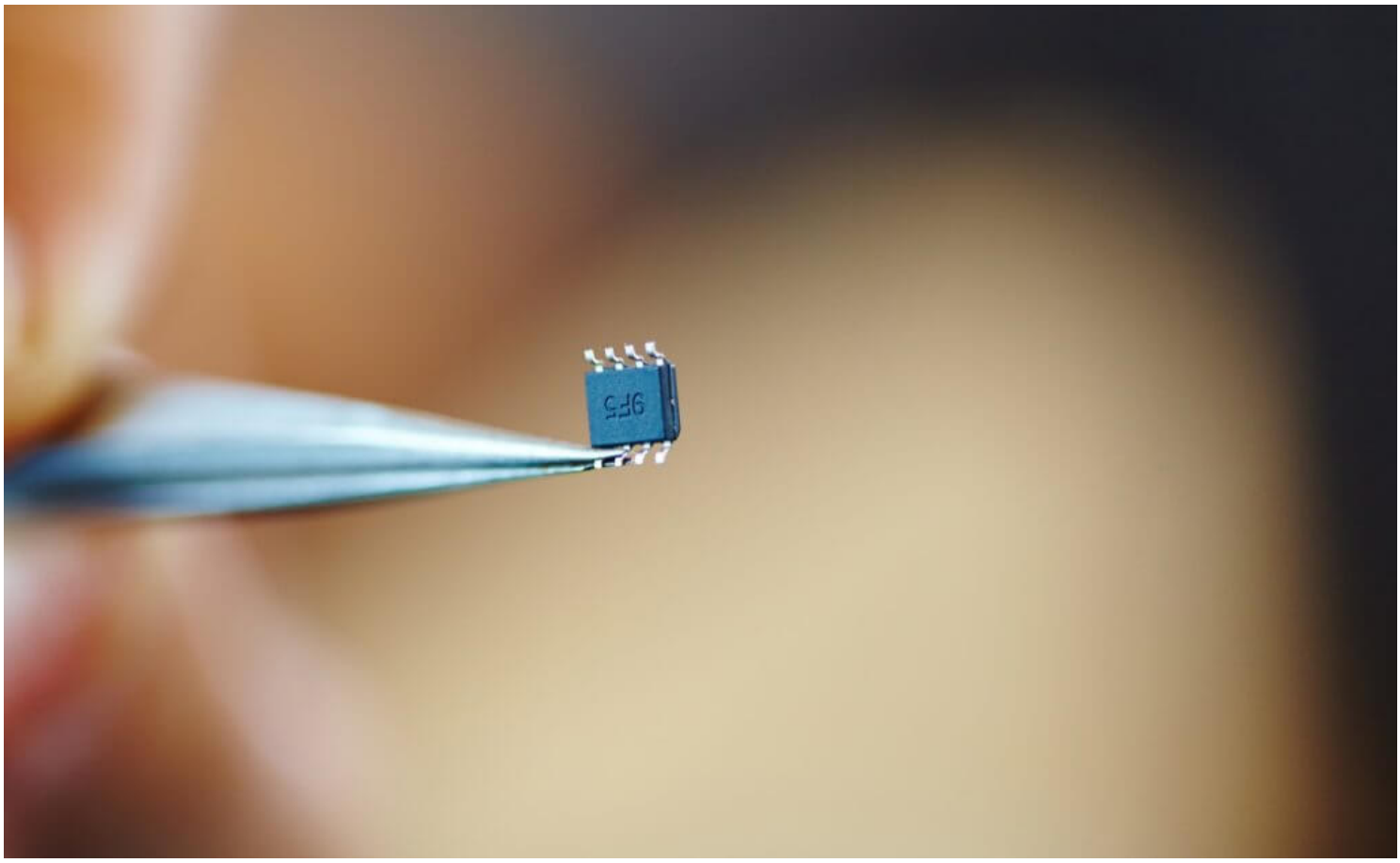
Microchip implants: A legal battle waiting to happen - AvvoStories

Tuesday, August 29 2017, 10:39 AM



Microchip implants: A legal battle waiting to happen

PRIVACY, BUSINESS, MONEY, NEWS, RIGHTS

Aug 20, 2017

By Gemma Alexander

13 1

Science fiction has predicted it for decades: In a brave new world, the corporate surveillance state will microchip humans for constant tracking and data collection, and people won't even protest.

They just didn't know that people would be getting the implants to facilitate snack food purchases.

New world, new tech

Three Market Square (also known as 32M) is a business based in River Falls, Wisconsin that provides technology for breakrooms and micro-markets, with a subsidiary called Turnkey Corrections that provides technology services to prisons. 32M partnered with Swedish microchip developer BioHax International to develop a radio frequency identification-enabled (RFID) subdermal microchip for its employees.

32M is the first company in America to implant employees with microchips. Over 50 of the company's 92 Wisconsin-based employees volunteered to have a microchip the size of a grain of rice injected between their thumb and forefinger.

Why? The chip replaced their company key card, which allows employees to access secure areas of the building, log in to their computers without typing a password, and purchase snacks at office vending machines.

What could go wrong?

The chips are physically safe; pets have been microchipped for years, and the FDA approved implantable chips for humans in 2004.

Privacy is another question. The current generation of microchips do not have GPS capabilities, and their encrypted data is far less detailed than the average cell phone. But encryption is not a guarantee against hacking, especially as more sensitive and valuable data is added. CEO Todd Westby already foresees using RFID for "unlocking phones, sharing business cards, storing medical/health information, and used as payment at other RFID terminals."

Critics point out these functions can already be filled with external options, like cell phone apps. Another issue, as Michael Zimmer, director of the Center for Information Policy Research at the University of Wisconsin-Milwaukee, points out, is lack of user control. "I can't turn it off and I can't just take it out and put it back in. I think that's a fundamental change in the way we control what access people have to our bodies."

Add while the participants were all technically volunteers, there's still an employer-employee power dynamic at work. With no more than the employer's word on what kind of data will be collected, how safely it's encrypted, or how the company will use what it learns, employees could find themselves quite vulnerable.

Pre-emptive protections

Some elected officials are not waiting for abuses before acting. Tina Davis, a member of the Pennsylvania House of Representatives, has proposed an Employee Subdermal-Microchip Protection Act that would prohibit employers in the Keystone State from requiring employees to accept microchip implants as a condition of employment.

Five states—California, Missouri, North Dakota, Oklahoma, and Wisconsin—already have enacted employee microchip protection laws.

The future is here, but it's not clear

Not everyone is worried. Tesla founder Elon Musk is an implant fan, and in the hacker subculture, some "grinders" are already getting implants just for fun. Whether implanting key cards is the first step toward a brave new world or corporate dystopia, a host of technical, ethical, and legal questions remain to be answered.

Tagged privacy, safety, small business

Leave a comment