Employee Injected Microchips:

Evaluating the Concerns in Privacy and Health

Matt Held

Edgewood College

The act of tracking employees has been happening with or without their knowledge for many years. Henry Ford had a sociology department that investigated workers' home lives and personal habits. (Chory, Vela, & Avtgis, 2015) There is a new type of technology that has been becoming increasingly more common, called microchips. This technology empowers employees to inject a small "rice-sized" chip into their body to give them secure access to doors, copy machines, their computers, phones, company transportation, and much more. While concerns revolve around personal privacy and health (Rodriguez, 2019) (Lai, Chan & Singh, 2016), it is important to look at what current privacy issues exist in the workplace, then look into how much more of an impact a microchip would have on these concerns.

Current Privacy Concerns in the Workplace

Privacy in the workplace has been a concern for employers and employees alike. Currently, in mobile workplace environments, “all…52 private companies and public organizations that participated in the study used two or more types of field technology.” (Tranvik & Bråten, 2017) An article written by Susan Park in the American Business Law Journal looks into the experience of interviewee Justin Basset as he was pressured to provide Facebook credentials during an interview. (Park, 2014) Not only does this violate workplace privacy, but it also creates a lack of trust between the employee and the employer. The request to access confidential information from an interviewee caused employee privacy to be compromised. Recently more than ever employers are also asking for privacy-invasive information from employees that have been with the business for a long time.

Park discusses the story of Robert Collins, a “Maryland Department of Public Safety and Correctional Services employee.” Robert was previously hired with the company but took a leave due to a death in the family. During his reinstatement interview, his supervisors asked for

his Facebook login information to make sure he was not involved in any gangs. (Park, 2014) Additionally in Montana, Illinois, Virginia, and Michigan there have been reported incidents of social media and email passwords being asked for on employment applications. (Park, 2014) It seems that this type of tracking has already reached high popularity. According to a survey, "70% of the employers were reported using social media for screening of the candidates." (Trivedi & Trivedi, 2018) This information is used to search for deeper information about the employee especially on non-public platforms like email. Since passwords are commonly reused, it makes it easy to be concerned about what other online resources employers could access once they have the employee's password.

According to an article in the Employee Responsibilities & Rights Journal by Rebecca Chory, Lori Vela, and Theodore Avtgis, individuals believe that they control their information and interactions. Therefore, when employee tracking solutions are used, they "feel their privacy has been invaded." (Chory, Vela, Avtgis, 2016) It seems that monitoring in the workplace is not merely managed by privacy laws alone. "Aggressive monitoring systems may be acceptable in a court of law yet rejected by valued employees seeking an environment of mutual respect and trust." (Chory, Vela, Avtgis, 2016) Nevertheless, as the workplace shifts into new generations, a focus on the boundaries of personal and work-life might change.

According to the Global Journal of Enterprise Information Systems, Vikas Trivedi and Vaishali Trivedi, claim that employers will want to track information more often with a new workforce coming in. This is because of the concerns of the "digital craze." Digital craze is the concept that some generations might be blind to the idea that some parts of lives shouldn't be shared freely on social media. "Digital craze among young employees may make them sometimes blind to the dangers of sharing sensitive information about their employers or

organizations, which may result in troubles for the firms in question." (Trivedi & Trivedi, 2018) An aspect of this revolves around an increase of wearables. Wearables in the workplace bring a concern to employees as workplaces are more often offering programs that require employees to wear one of the company's trackers to gain insurance discounts depending on how many steps they take, for example. These concerns stretch farther than just during the workday. A major concern is that employees could be tracked or listened to at home. Additionally, with employers getting closer to being able to access health information, employees might not have an equal chance at using personal time or sick days. (Trivedi & Trivedi, 2018) Due to recent innovations, it appears that companies have already engaged in privacy concerning tactics.

For example, "Amazon monitors its employees utilizing GPS tags while they are inside the warehouse." (Trivedi & Trivedi, 2018) By doing this, Amazon makes it easy to tell if an employee left work early, has been stationary conversing with an employee, or other areas of concern. (Trivedi & Trivedi, 2018) Other companies have used technology by the company Humanyze, which records and analyzes employee data, like phone calls and emails to determine their tone of voice. This data can be looked at on a large scale to track an employee's expected satisfaction and their effectiveness in communication and teamwork. Additionally, this analysis software can show change over time as the company changes policies or employee turnover occurs. (Trivedi & Trivedi, 2018) Because Humanyze can track every aspect of an employee, employees should be concerned with false positives just based on their personality and the inaccuracies of current artificial intelligence (AI) systems. Now that the basics of current employee privacy concerns have been covered, looking into concerns about microchip technology specifically is the vital next step.

Concerns of Microchips in the Workplace

People often think of microchips as a “Big Brother” technology, something that is going to provide the government or an employer with each step someone takes or each thought someone thinks. (Katina & MG, 2013) In reality, microchips are used to simplify actions done every day. Some items that microchips can replace are door keys, ATM cards, gym-locker cards, bus tickets, and copy machine authentication cards. Microchips are injected by a needle normally in the skin in between the thumb and index finger. (Walt, 2019) While this technology is not as common in the United States currently, a Wisconsin company, Three Square Market has adapted this technology. Fifty employees decided to opt-in. (Bowerman, 2017) This microchip technology often brings concerns of employees "not having a choice" if they want a microchip installed. The Wisconsin company has made this an opt-in program and will also pay for the procedure. (Menegus, 2017) Even with this in mind, employees still worry about their private data.

One aspect of personal data is GPS tracking. Todd Westby, CEO of technology company 32M, says, “the chips don't include a GPS component." Though tracking someone is different than collecting data that identifies what they do daily. This could include letting employers view information such as “often [an employee] take breaks or use the bathroom, what kind of snacks they buy, and so on.” (Dockrill, 2017) Even that this is not currently implemented in the microchip plan, as technology evolves and more of this information would become accessible to employers. “It's possible that handing over even that level of information to your employer could one day pose problems – not to mention how the privacy issues could swell as the technology evolves.” (Dockrill, 2017) It is important to have checks and balances for making

sure that employers do not abuse this system. With this in mind, employer privacy is only one aspect of the puzzle.

If microchips get to the point of being used worldwide and across industries, it could be a concern about who would have access to private data with a “swipe of the hand.” This brings up the fear of "Hacking." Unlike most technology, microchips cannot be accessed without physically being near the microchipped hand. Westby describes the risk of hacking as “almost non-existent because it's not connected to the internet. The only way for somebody to get connectivity to it is to basically chop off your hand.” (Dockrill, 2017) What if someone did have unknown access near a hand, like putting a scanner near accessible places where people would typically place their palm, on a handrail in a staircase, for example. Westby claims that this is not a concern. “There's really nothing to hack in it because it is encrypted just like credit cards are.” (Dockrill, 2017) So in theory, no one would be able to access this information without authorization from the chip due to the encryption of the data, but what about data that could be stored in other locations.

According to Epicenter's CEO, Patrick Mesterton, "[data] is stored in the microchip, and it communicates with a device (reader, mobile phone, etc.). “No data is stored with Epicenter or monitored.” (Menegus, 2017) However, the concern is not necessarily what the data would be used for during this “beta phase” but how the company would decide to use this data in the future. For example, collecting data that an employee consistently buys lunch in the cafeteria at noon, and goes to the vending machine at 3, gives the employer a good indication of where the employee could be at a given time, or how much time the employee spends away from their desk. (Dockrill, 2017) This shows the importance of reading the terms and conditions and making sure that the employer is transparent on how this data will be used.

Adam Levin, chairman, and founder of data protection firm CyberScout, says that “Many things start off with the best of intentions, but sometimes intentions turn.” In theory, this means that your data should never be accessible to anyone but yourself, but only time will tell if that stays true. Therefore, it is essential to look at the implications of an employee having their microchip removed. If employees later do decide that they would like their chip removed, they do have that option without any additional charge. (Dockrill, 2017) Just having an opportunity to remove the chip does not encompass all of the possibilities that could affect an employee’s further use of microchips. “What provisions, if any, are in place to remove or disable the chips when someone gets fired, quits, or wishes to unenroll?” (Menegus, 2017)

Levin seems to think that companies and people are jumping into microchips too soon. “We've survived thousands of years as a species without being microchipped, is there any particular need to do it now?” (Dockrill, 2017) Without a clear list of pros for microchips, it is difficult to see if the cost of privacy for the employees and the financial loss for the employer is worth it. It is also vital to investigate other causes of financial and family burden, like health concerns, specifically regarding skin radiation.

With the advancement of technology, the concerns around cancer caused by radiation increases. According to a study posted by the International Journal of Radiation Biology, microchips could have the opposite effect on human cancer cells. It is first essential to understand the basics of how passive chips work. "A passive RFID microchip absorbs energy from an external source and emits a radiofrequency identification signal which is then decoded by a detector.” (Lai, Chan & Singh, 2016) The study showed that this energy transfer caused cancer cells to die. “The energy effectively killed/retarded the growth of the three different types of cancer cells.” (Lai, Chan & Singh, 2016) The killing of cancer cells is appreciated, but how

about when the microchip will not be active, which happens to be most of the time. The study found that “an inactive microchip and energy from the external source had no significant effect on the cells. (Lai, Chan & Singh, 2016) This is important because the microchip will be in an inactivate state most of the time which also seems to improve skin health. With both health and privacy concerns considered, looking into how these concerns relate to current privacy issues helps conclude if microchip technology is a threat to workplace privacy.

Microchips Compared to Current Privacy Issues in the Workplace

First, looking into employers gaining access to employee passwords, microchips are not a threat to this type of privacy violation, as microchips do not have personal data contained on them. The chips are currently used to unlock doors, pay on vending machines, and print from printers. (Menegus, 2017) These are routine workplace tasks that one might alternatively get a ID card or key to perform.

Furthermore, this technology could advance to have new features, like private password storage, for example. This is where encryption and data storage come in. Companies are unable to read the data without the correct setup on the microchip and reader.

The same goes for the ability to access a “protected location” that has this data stored in it. The chip is not connected to the internet and is therefore basically impossible to hack. (Jarvis & Francis, 2017) Also, the information on the microchips is encrypted, just like credit card information is. Therefore, any information retrieved from the card is not usable. In certain countries, microchips are being used for things like ATM cards and gym lockers. (Walt, 2019) This starts to decrease the gap between being an employee tool vs. a life tool that your employer has access to. Looking at it from this perspective, it makes it well-defined about how an employer could learn more about you than just when one takes a lunch as discussed before.

Therefore, at this point it seems that microchips are a privacy risk to personal information and tracking until employers better reinforce what they can access. Because at that point, if the employer paid for the microchip injection, then the employer would be the one who owns it.

Another concern of employee privacy revolves around employees being tracked outside of the workplace. A way of this occurring is spying through wearables and GPS based tracking. Starting with wearables, as discussed, microchips are passive devices, that can only transmit information to a receiver, and are not connected to the internet." (Dockrill, 2017) This removes the concerns of employers listening in on personal conversations and shows the lack of connection between wearables as they are known, and the upcoming world of microchips.

Because microchips have no external connections (i.e., WiFi and Bluetooth), GPS tracking is not possible with microchips as they do not have a power source. They get all the power they need just from the reader itself. Some argue though that employees need to watch out to make sure that companies will not release "a new version of the microchip" that would allow employers to track employees through a form of GPS or Bluetooth. (Dockrill, 2017)

Weighing the pros and cons, it seems that microchips are not as much of a threat as the software and data collection that surrounds them. First off, with the lack of standalone microchip connectivity, microchips do not seem to be a direct risk in user privacy or tracking. Secondly, microchips seem to not cause skin harm but instead improve skin health, as it could one day have use for cancer treatment. (Lai, Chan & Singh, 2016) Though the long-term effects of microchips are not yet known, the only way to advance the technology is if employees take the risk like was done with cell phones, to develop and grow the technology. Though innovation is a two-way road, if employers are misusing this data and not giving employees a choice in adopting this technology, employees will not find the convenience to be worth the risk. Instead, if employers

make open and honest policies that empower the employee to use the technology to enhance their life, then microchips might succeed just like the innovation of the cell phone.

References

Areheart, B. A., & Roberts, J. L. (2019). GINA, big data, and the future of employee privacy. *Yale Law Journal, 128*(3), 710-790. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN =134459435&site=eds-live&scope=site

Chory, R., Vela, L., & Avtgis, T. (2016). Organizational surveillance of computer-mediated workplace communication: Employee privacy concerns and responses. *Employee Responsibilities & Rights Journal, 28*(1), 23-43. Retrieved from https://doi.org/10.1007/s10672-015-9267-4

Dockrill, P. For the first time, a US company is implanting microchips in its employees. *Science Alert.* Retrieved from https://www.sciencealert.com/for-the-first-time-a-us-company-is-implanting-microchips-in-its-employees

Lai, H. C., Chan, H. W., & Singh, N. P. (2016). Effects of radiation from a radiofrequency identification (RFID) microchip on human cancer cells. *International Journal of Radiation Biology, 92*(3), 156-161. Retrieved from https://doi.o

rg/10.3109/09553002.2016.1135264

Bowerman, Mary. (2017, July 24). Wisconsin company to install rice-sized microchips in employees. *USA Today.* Retrieved from https://www.usatoday.com/story/tech/nat

ion-now/2017/07/24/wisconsin-company-install-rice-sized-microchips-employees

/503867001/

Menegus, B. (2017). Company offers free, totally not creepy microchip implants to employees, *Gizmodo*, Retrieved from https://gizmodo.com/company-offers-free-totally-not-creepy-microchip-impla-1797190619;

Michael, K., & Michael, M. G. (2013). The future prospects of embedded microchips in humans as unique identifiers: The risks versus the rewards. *Media, Culture & Society, 35*(1), 78-86. Retrieved from https://doi.org/10.1177/0163443712464561

Park, S. (2014). Employee internet privacy: A proposed act that balances legitimate employer rights and employee privacy. *American Business Law Journal, 51*(4), 779-841. Retrieved from https://doi.org/10.1111/ablj.12039

Rodriguez, D. A. (2019). Chipping in at work: Privacy concerns related to the use of body microchip ("RFID") implants in the employer-employee context. *Iowa Law Review, 104*(3), 1581 -1611. Retrieved from https://edgewood.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=135811112&site=eds-live&scope=site

Tranvik, T., & Bråten, M. (2017). The visible employee - technological governance and control of the mobile workforce. *Management Revue, 28*(3), 319-337. Retrieved from https://doi.org/10.5771/0935-9915-2017-3-319

Trivedi, V. (2018). Blurred work - life frontiers: A paradigm shift in employee social networking privacy. *Global Journal of Enterprise Information System, 10*(1), 38-44. Retrieved from https://doi.org/10.18311/gjeis/2018/20925