Issues of uberveillance in the workplace

ChallengesFaced by ICT Professionals: Uberveillance

Introduction

Michael and Michael (2007) state that uberveillance uses cutting-edge surveillance technology to identify, locate, and track individuals. It is omnipresent and based on pervasive electronic devices such as computer chips that are implanted into the body. The idea of uberveillance brings up various concerns about privacy, ethical, and human rights. This is because these devicesmonitor individualsand compel them to provide detailed information about themselves, their likes, dislikes, habits, behaviours, and preferences (Chirgwin, 2015). This could lead to abusive or dangerous situations if such information falls into the wrong hands.

Privacy and uberveillance

Several issuescome up concerning uberveillance at the workplace. Michael (2012) states that electronic and monitoring surveillance practices have significantly increased in the last years to encompass all aspects of life, including the workplace. Emails, social networking, and LinkedIn are some examples of communication flows in and out of a workplace. This e-communication comes with some potential risks to the employers and employees because of the need for extended permissible authority for surveillance, the growth of relational databases, and a business that is committed to filling them (Michael & Michael, 2014). ICT professionals use these sites and media forms to communicate with clients and colleagues. If they are under uberveillance, their activities and actions could be tracked and exploited to get information from them that could potentially harm them and their company.

As Michael and Michael (2009, p. 4) state, thesesurveillance technologies are used mainly on the common people and not onrulers, leaders, or people of influence. It is only used on the leaders incases of blackmail or industrial espionage. At the place of work, it is mostlythe employees who are subjected to uberveillance; by their superiors. Everyoneneeds some privacy (Michael & Michael, 2009 p. 4), but uberveillance makesthis privacy obsolete. The ICT employees need to have a modicum of privacy evenif they are on work premises and using work equipment and resources. However, working for someone or a corporation means that the employees should alsoaccept that their privacy will be invaded. The use of uberveillance at workwould invade employee privacy completely and subject them to unnecessaryscrutiny on their private and public lives. Uberveillance would enableemployees to follow an employee's life even when they are not at work. Information gathered could be used negatively or positively against them. Kurkovsky et al. (2011) shows how employers could use an RFID tracker to keeptrack of employee location. This can be beneficial if the tracker helps toimprove job productivity. However, it should not be used to monitor theemployees in order to micro-manage their time and activities, as this coulddiscourage them.

Impact of uberveillance on work productivity andefficiency

Uberveillance devices such as microchips canenable the ICT professionals to access work-related technologies like printersor scanners, log onto their computers, and open secure doors (Mazanov, 2017). It can also be used as a cure or remedy for forgetfulness even in the workplacewhen an employee forgets where they placed a project or how they performed acertain task. A

microchip would enable employees to swipe their security and IDcards into the work building, and to pay for food and other services in thework space (Astor, 2017). Michael and Michael (2014) however see the need formore research on the use on uberveillance at the workplace. Even though microchipping aids in automating payroll systems and the effective use of onlinecommerce practices, it could be costly and unhealthy to embed microchips inemployees and other individuals (Mazanov, 2017).

Widespread use of uberveillance and itsassociated devices could change the way employees work, perform tasks, and evenenter the profession (Joint Workshop, 2012). When employees are aware that theyare being monitored, they could either become more motivated to work, or feelstifled in their environment. This can limit their imaginations and placelimits on their natural impulse to act spontaneously and to freely use theirimaginations for company and personal benefit. They also become constrained inthe use of words and expressions. Their creativity and relaxation levelsreduce, causing them to work below optimum and with a lot of anxiety that couldbring negative results for the company. However, uberveillance devices, if usedproperly, could help to monitor their levels of stress and the onset ofwork-related illnesses and ultimately facilitate earlier return to work afteran illness (Joint Workshop, 2012 p. 5).

Uberveillance and health issues

Many ICT professionals are nervous about havinga device implanted into their bodies because they still do not know much aboutthem and their effects and capabilities. According to experts, micros chips andother devices do not have tracking abilities (Sheppard, 2017). However, theyare aware that

these devices will be a major part of everyday life in thecoming years and will be fully integrated into their personal and professionalrealms. Health issues and injury lawsuits could arise if the implant migratesto another part of the body or if it becomes infected (Astor, 2017). This couldlead to absenteeism at work as employees require treatment or hospitalizationfor corrective measures to be performed.

The U. S Food and Drug Administration (2014)states that it is unaware of any side effects from RFID implantation in humanbeings, although there are concerns about their effect on medical devices. Michael and Michael (2014 p. 281) state that research has shown how microchipshave caused cancer in animals, and further recommendations and research isneeded for use in human beings. If employees get such implants and they end upwith adverse effects, then their productivity and ability to work becomescompromised.

Uberveillance and security

Implants and chips are usually encrypted, andare thus susceptible to hacking or reading by third-party scanners. Individualscould secretly access information from these devices and clone the signal togain access in order to impersonate the chipped individual (Byles, 2006). Thiscould affect ICT employees as they often deal with sensitive companyinformation that could be hacked by competitors or blackmailers for companyespionage. It is thus not secure to use uberveillance on employees who dealwith sensitive business data as their lives could be put at risk. Byles (2006)also states that such a breach of security could result in problems forbuilding or computer access by locking individuals out of their work place, secure rooms, or their designated work areas.

Uberveillance will lend individuals to evengreater scrutiny and surveillance, resulting in a total loss of freedom. Theelectronic and technological world are fragile, therefore uberveillance couldincrease the insecurity of data and information used on such devices at theworkplace. Michael (2017) states that uberveillance is impelled by the need forcontrol from superiors in order to scrutinize their juniors' lives andthoughts. This could apply in the workplace as employer's desire to control allthe activities of their employees, regardless of whether this could harm theemployees. Employers might believe that uberveillance increases security atwork (Michael, 2017), but this could be the opposite if the technology breaksdown or is used for criminal activities.

Legal and ethical implications of uberveillance

Employees should be made aware of and freelyconsent to uberveillance, and if they so wish, they can withdraw this consent(Sheppard, 2017). Pressure to comply can make employees resign, claimingconstructive dismissal. Monitoring practices should be under the laws of dataprotection and human rights policies, with employers conducting careful impactassessments prior to introduction of uberveillance. The ICT employees need tobe informed why it is valid and justified to monitor their movements, logs, andactivities at the workplace.

In addition, there could be religious orpersonal beliefs that prevent employees from being implanted with uberveillancedevices (Sheppard, 2017). If these are violated, the business could face alawsuit. To mitigate this, data protection regulations should be prepared andsigned by employees prior to implantation to ensure their decision is informedand

consent is free (Michael & Michael, 2010 p. 10). Although employee monitoringsystems are commonplace in businesses, uberveillance can be seen as crossing amoral, political, and legal threshold.

Employers and others who require their staff touse uberveillance devices must differentiate between active and inactiveimplants, reversible and non-reversible ones, and offline and online ones(Michael & Michael, 2010 p. 10). They should ensure that employee dignity ismaintained so that the employees are not manipulated or controlled remotely asa source of information. Uberveillance should be permitted if there isjustification and necessity for its use at the workplace and there are nobetter methods of acquiring information without invasion of privacy. Suchsurveillance methods must thus be specified in legislation, and approved and monitoredlegally (Michael & Michael, 2010 p. 11)

Conclusion

Research shows that there is various security, privacy, ethical, health, and legal implications for the use of uberveillanceat the workplace. Even though it can make the work of employees easier in someways, its use can also be detrimental in their wellbeing and productivity. Ifnot properly inserted, health problems could arise and make the employeesunable to work. The uberveillance devices must be kept secure to prevent systemhacking and even espionage at the workplace, because ICT professionals tend todeal with sensitive and classified information. Care must however be taken toensure that employees being surveilled have given consent and are aware of theimplications of the practice.

Uberveillance is still developing, it is aninevitable part of the future that will be quickly embraced. It will becomemore incorporated into the workplace and help to improve productivity andemployee retention if used appropriately. Technology and uberveillance howevermust be used ethically and humanely because they ultimately convey theintentions of the creators, who might have created them for their personalgain.

References

Astor, M2017, " Microchip Implants for Employees? One Company Says Yes", *Nytimes. com* , viewed 20 August, 2017, .

Byles, I2006, " Health-care chips could get under your skin", *Medicalxpress. com* , viewed 20 August, 2017, .

Chirgwin, R2015, " Welcome to ' uber-veillance' says Australian PrivacyFoundation", *Theregister. co. uk* , viewed 20 August, 2017, .

Joint Workshop 2012, *Human enhancement and the future of work* , JointWorkshop, pp. 43-45, viewed 21 August, 2017, .

Kurkovsky, S, Syta, E & Casano, B 2011, Continuous RFID-enabled authentication: Privacy implications, *IEEE Technology and Society Magazine* , vol. 30, no. 3, pp. 34-41

Mars, C 2014, ICT staff ' losing sleep' overwork pressures, Public Technology, viewed 21 August 2017, .

Mazanov, J 2017, ' Intersecting performanceenhancing smart technologies, health and social science', Science Direct, vol. 5, no. 3, pp. 87-88

Michael, K 2012,“ Workplace Privacy”, *Uberveillance* , viewed 22 August, 2017, .

Michael, M. G & Michael, K 2007, *A note on “ uberveillance”.* In K. Michael& M. G. Michael (Eds), The Second Workshop on the Social Implications ofNational Security: From Dataveillance to Uberveillance and the Realpolitik ofthe Transparent Society, pp. 9-25 Wollongong: University of Wollongong

Michael, M 2016, *TheParadox of the Uberveillance Equation* , IEEE, viewed 22 August, 2017, .

Michael, M &Michael, K 2009, *Uberveillance: Microchipping people and the assault onprivacy* , viewed 23 August, 2017, .

Michael, M &Michael, K 2010, *Toward a state of Uberveillance* , IEEE Technology andSociety Magazine, viewed 23 August, 2017, .

Michael, M. G & Michael, K 2014, Uberveillance and the social implications of microchip implants: Emergingtechnologies. IGI Global, Hershey, PA.

Sheppard, D 2017, Microchipping workers: Whatare the moral, practical and legal implications? Personnel Today, viewed 22August 2017, .

U. S. FDA 2014, Radio Frequency Identification(RFID), viewed 22 August 2017 .