Do Privacy Concerns Prevent Employees' Acceptance of Smart Wearables and Collaborative Robots?

Alexander Richter[1]

Abstract: During the digitization of workplaces, companies are increasingly using smart wearables as well as collaborative robots. This technological progress can contribute to higher productivity and efficiency in manufacturing processes, as they assist employees in carrying out their work. This changes the way employees interact and collaborate with their working environment and robots. When companies utilize smart wearables and collaborative robots in their processes, employees are exposed to various privacy issues, which may lead to privacy concerns and may reduce the acceptance of such devices and robots. Thus, the presented PhD research project aims to understand the employees' privacy concerns and address them.

Keywords: Privacy; Employees' Acceptance; Smart Wearables; Collaborative Robots; Smart Workplaces

1 Introduction

Employees' work is changing in factories and other industries. Companies digitize manufacturing processes to optimize workplaces and operations to achieve higher productivity and greater efficiency. For this, smart wearables have the potential to contribute in increasing productivity. Therefore, an increasing number of companies are equipping their employees with smart wearables [Sc16] to improve workers' productivity [Sp13; We15], health [Go17; Li14], and safety [CHL17]. Another essential aspect in industrial processes is human-robot collaboration [Ro17; SM17], as humans and robots can collaborate in an increasing number of tasks due to a new generation of robots and sensors [Ro17; SM17]. However, to facilitate human-robot collaboration, the separation of their workspaces need to be eliminated [Ro16; SM17]. Therefore, different sensors to enhance employees' safety must be embedded in collaborative robots.

However, the potential benefits which entail from such devices and robots are always offset by risks that may affect the employees' privacy. For example, these risks arise from wearing such devices or the interaction with robots by the respective employee due to the possibilities to collect employees' data with the devices or robots. Various authors have already shown that the use of different sensors and devices enhance the possibility to endanger users' privacy [Sh15; WLR15]. Examples include reading sensor data, such as the gyroscope or the

[1] Institute of Computer Science, University of Göttingen, Goldschmidtstr. 7, 37077 Göttingen, Germany
richter@cs.uni-goettingen.de

doi:10.18420/sicherheit2020_14

acceleration sensor. These data make it possible to determine, i.e., users' physical activities. Equal potential risks are also able to arise in the corporate context. For example, this can be seen in the scandal of the Tesco company, where employees were equipped with digital wristbands that allowed managers to find out how much the employees worked [AF13].

Both technologies are components of recent and future digitization of workplaces, as they can enhance productivity and employees' efficiency. Due to the embedded sensors, employers can collect, analyze, and draw inferences about the employees, especially, when they use them for entire shifts. Moreover, combining several sensors' data might give employers more insights regarding employees' sensitive data, for instance employees' health, job performance, etc. Therefore, this PhD research project examines the discrepancies between employers and employees, address them and potentially contribute to increase the acceptance of digitized processes. Thus, the main goal of the project is to first analyze whether the employees' privacy concerns influence their acceptance of such devices. Moreover, it aims to analyze whether increasing the data collection transparency control mechanisms, can improve employees' acceptance to mitigate such employees' concerns.

2 Related Work

Previous research can be classified into three categories: (1) employees' acceptance, (2) privacy concerns, and (3) proposed solutions. The first category includes employees' acceptance surveys conducted in a corporate context, such as [CHL17; Ja19; LHZ19]. Choi et al. identified different influence factors, like perceived usefulness, social influence, and perceived privacy risks, which have an impact on the adoption of smart wearables for occupational safety and health management. Beside employee beliefs, employees' acceptance can also be affected by job position in a company or experience with such devices [CHL17; Ja19]. Existing work is mostly based on a specific use case. Jacobs et al. investigated factors that are related to the organizational settings, the individual employee, and the purpose or use case at the workplace.

In the second category, privacy concerns are identified and classified in different ways in existing works. These privacy concerns are closely related to the embedded sensors with the ability to sense, collect, and store data [MC15] and increase with a physical and temporal context [Ra11]. Furthermore, users are not able to understand potential threats about collected data about behavior disclosures and context from measurements by sensors, unless these are their own data [Ra11]. Besides, previous work mentioned general fears from employees in the context of workplace environments. These include the fear of being under surveillance or tracked by the employers [CHL17; DNC18; SSC18] or the risk that the devices record sensitive information [CHL17; DNC18]. This, especially with regard to surveillance and monitoring, may have a negative impact on job satisfaction and also in the level of employees' stress and may lead to a deterioration in productivity [Me03; TLA18].

For the latter category, different authors propose rules relevant to workplace surveillance [Sa06] or offer recommendations to maximize the positive effects of electronic performance monitoring and to minimize negative ones [TLA18]. These rules include several points such as informing the employees about the data that are collected or accessed as well as how employees can access and correct the information [Sa06; We15]. Thus, employers should be transparent about monitoring processes and use the insights for learning and developing rather than for preventing unwanted employees' behavior. Moreover, employers should monitor only work-related behaviors [TLA18]. Furthermore, employers must take reasonable measures to protect information from misuse, loss, unauthorized access, modification or disclosure [Sa06]. However, these are only general recommendations for employers. A general approach for employers to give employees the ability to gain access to gathered data to comply with the GDPR and thus to enhance employees' privacy is hence still missing.

To the best of our knowledge, there is no previous work that focuses on the following two issues: (1) analyzing employees' privacy concerns arising by the adoption of smart wearables or the collaboration with robots, based on their knowledge regarding possibilities of sensor readings as well as (2) developing an approach allowing employees to get more transparency and control over the collected data by wearables and robots especially w.r.t. the threats related to embedded sensors in smart workplaces. Therefore, our entire research work focuses on the above-mentioned issues.

3 Research Questions and Methodology

The basis of the PhD research project relies on analyzing existing research papers, which address the key topics of smart workplaces, smart wearables, collaborative robots, control, transparency, and minimization of data as well as various technology acceptance models in the context of privacy.

In this work, we will analyze the impact of employees' privacy concerns on their acceptance to use smart wearables and collaborative robots as basis for the development of an approach to protect employees' privacy. In more detail, we will consider the following research questions.

Which privacy risks prevent the use of smart wearables or the collaboration with robots? — We will start by conducting, a structured literature review. Likewise, some in-depth case studies with helpful industry partners shall be conducted to get a closer look into processes with such devices and their implementation and use in companies. Core issues are risks and threats that may arise from these technologies and thus affect individuals' privacy. For a better understanding of existing privacy risks and threats, we will analyze and identify the general threats and risks of such devices, and the included sensors. Likewise, it includes sensors or techniques that threaten individuals' privacy.

Which employees' level of knowledge regarding privacy risks result in acceptance problems? — Regarding the previous insights, privacy concerns arising from employees' level of knowledge (knowledge or ignorance), need to be examined. Knowledge implies that employees are aware of risks for their privacy, which can result in the rejection of new technologies since they can understand the technology's data processing and occurring consequences. In comparison, ignorance implies that those rejection results from the fear based on a lack of knowledge about these potential risks towards their privacy, as they are not able to grasp how data collection or processing works or which consequences results from this data, for instance. Thus, these are two antagonistic causes from which privacy concerns may arise. For this purpose, a qualitative and quantitative survey shall contribute to identifying these concerns. Therefore, a first targeted and direct semi-structured interview with employees will be held and provide the first insights on perceived privacy risks and threats. Based on the qualitative interviews, a quantitative survey will be conducted that verifies the insights of the interviews and will confirm or reject their significance. For this purpose, the participants are presented with various benefit and risk scenarios, for instance. From the conducted surveys, an analysis of the ensuing employees' acceptance problems is required about the use of those devices in the company context. For this purpose, the technology acceptance models such as Technology Acceptance Model (TAM) or Unified Theory of Acceptance and Use of Technology (UTAUT) will be analyzed and applied to the research problem.

Which information or conditions influence employees' acceptance? — By means of a survey, information and conditions shall be identified, which may positively influence the employees with respect to the adoption and use of smart wearables or the collaboration with robots. For this, it is necessary to verify, whether the control or transparency of the collected employees' data as well as the data minimization, e.g., by pseudonymization affects the deployment of these devices mentioned above. Therefore, it must be clarified to what extent to control, transparency, and data minimization are understandable in order to help the employers to respect the GDPR compliance and implement mechanisms to improve employees' privacy.

How do solutions need to be implemented in companies to ensure and enhance employees' privacy? — Based on the results obtained, an approach shall be formulated with the aim to improve employees' privacy. This can be achieved through control mechanisms and/or transparency of processes by the management but also through systems, which have already required to implement regarding the GDPR. However, companies need effective approaches to fulfill the requirements. Thereby, the employees' acceptance to use smart products could be enhanced. Afterwards, an evaluation of the proposed solution would take place by means of user studies.

4 Summary and Expected Contributions

This PhD research project aims to contribute in designing a model, e.g., an interface, that will enable employees to gain more transparency, access, and control over their personal

information generated within the company, especially in presence of smart devices and collaborative robots. For companies to benefit from the above-mentioned advantages of the digitization of workplaces, our proposed approach could contribute to reduce employee's privacy concerns and consequently improve their acceptance.

References

[AF13] Applin, S. A.; Fischer, M. D.: Watching Me, Watching You.(Process Surveillance and Agency in the Workplace). In: Proc. of the 2013 IEEE International Symposium on Technology and Society (ISTAS): Social Implications of Wearable Computing and Augmediated Reality in Everyday Life. Pp. 268–275, 2013.

[CHL17] Choi, B.; Hwang, S.; Lee, S. H.: What Drives Construction Workers' Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health. Automation in Construction 84/1, pp. 31–41, 2017.

[DNC18] Datta, P.; Namin, A. S.; Chatterjee, M.: A Survey of Privacy Concerns in Wearable Devices. In: Proc. of the IEEE International Conference on Big Data (Big Data). Pp. 4549–4553, 2018.

[Go17] Gorm, N.: Personal Health Tracking Technologies in Practice. In: Companion of the 20th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW). Pp. 69–72, 2017.

[Ja19] Jacobs, J. V.; Hettinger, L. J.; Huang, Y.-H.; Jeffries, S.; Lesch, M. F.; Simmons, L. A.; Verma, S. K.; Willetts, J. L.: Employee Acceptance of Wearable Technology in the Workplace. Applied Ergonomics 78/1, pp. 148–156, 2019.

[LHZ19] Lotz, V.; Himmel, S.; Ziefle, M.: You're My Mate–Acceptance Factors for Human-Robot Collaboration in Industry. In: Proc. of the International Conference on Competitive Manufacturing (COMA). Pp. 405–411, 2019.

[Li14] Lingg, E.; Leone, G.; Spaulding, K.; B'Far, R.: Cardea: Cloud Based Employee Health and Wellness Integrated Wellness Application with a Wearable Device and the HCM Data Store. In: Proc. of the 1st IEEE World Forum on Internet of Things (WF-IoT). Pp. 265–270, 2014.

[MC15] Motti, V. G.; Caine, K.: Users' Privacy Concerns About Wearables. In: Proc. of the 18th International Conference on Financial Cryptography and Data Security (FC). Springer, pp. 231–244, 2015.

[Me03] Meyers, N.: Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals. In: Proc. of the 14th Australasian Conference on Information Systems (ACIS). Pp. 72–81, 2003.

[Ra11] Raij, A.; Ghosh, A.; Kumar, S.; Srivastava, M.: Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment. In: Proc. of the 29th ACM Conference on Human Factors in Computing Systems (SIGCHI). Pp. 11–20, 2011.

[Ro16] Romero, D.; Stahre, J.; Wuest, T.; Noran, O.; Bernus, P.; Fasth Fast-Berglund, Å.; Gorecky, D.: Towards an Operator 4.0 Typology: A Human-Centric Perspective on the Fourth Industrial Revolution Technologies. In: Proc. of the 46th International Conference on Computers and Industrial Engineering (CIE). Pp. 1–11, 2016.

[Ro17] Robla-Gómez, S.; Becerra, V. M.; Llata, J. R.; Gonzalez-Sarabia, E.; Torre-Ferrero, C.; Perez-Oria, J.: Working Together: A Review on Safe Human-Robot Collaboration in Industrial Environments. IEEE Access 5/1, pp. 26754–26773, 2017.

[Sa06] Sandy, G. A.: Workplace Privacy and Surveillance: A Matter of Distributive Justice. In: Proc. of the 17th Australasian Conference on Information Systems (ACIS). Pp. 69–79, 2006.

[Sc16] Schellewald, V.; Weber, B.; Ellegast, R.; Friemert, D.; Hartmann, U.: Einsatz von Wearables zur Erfassung der körperlichen Aktivität am Arbeitsplatz. DGUV Forum 11/1, pp. 36–37, 2016.

[Sh15] Shoaib, M.; Bosch, S.; Scholten, H.; Havinga, P. J.; Incel, O. D.: Towards Detection of Bad Habits by Fusing Smartphone and Smartwatch Sensors. In: Proc. of the 13th IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops). Pp. 591–596, 2015.

[SM17] Steil, J. J.; Maier, G. W.: Robots in the Digitalized Workplace. The Wiley Blackwell Handbook of the Psychology of the Internet at Work/, pp. 403–422, 2017.

[Sp13] Spath, D.; Weisbecker, A.; Peissner, M.; Hipp, C.: Potenziale der Mensch-Technik Interaktion für die effiziente und vernetzte Produktion von morgen. Fraunhofer-Verlag, Stuttgart, 2013, ISBN: 978-3-839-60563-9.

[SSC18] Schall, M. C. J.; Sesek, R. F.; Cavuoto, L. A.: Barriers to the Adoption of Wearable Sensors in the Workplace: A Survey of Occupational Safety and Health Professionals. Human Factors 60/3, pp. 351–362, 2018.

[TLA18] Tomczak, D. L.; Lanzo, L. A.; Aguinis, H.: Evidence-based Recommendations for Employee Performance Monitoring. Business Horizons 61/2, pp. 251–259, 2018.

[We15] Weston, M.: Wearable Surveillance – a Step Too Far? Strategic HR Review 14/6, pp. 214–219, 2015.

[WLR15] Wang, H.; Lai, T. T.-T.; Roy Choudhury, R.: Mole: Motion Leaks Through Smartwatch Sensors. In: Proc. of the 21st ACM Annual International Conference on Mobile Computing and Networking. Pp. 155–166, 2015.