Designing a Privacy Dashboard for a Smart Manufacturing Environment

Felix Mannhardt[1,2](✉), Manuel Oliveira[1,2], and Sobah Abbas Petersen[2]

[1] KIT-AR, London, UK
{felix.mannhardt,manuel.oliveira}@kit-ar.com
[2] SINTEF Digital, Trondheim, Norway
sobah.petersen@sintef.no

Abstract. In smart manufacturing environments sensors are collecting data about work processes. This data likely also contains references to actions of a single worker, which can be considered personal data. Privacy dashboards convey information on what personal data is stored by a system and provide means for users of a system to control what personal data is shared according to their needs. Dashboards put the control over their personal data in the hands of the users. However, to act as a trust building component, the dashboard needs to convey or mediate the trade-off between the user's privacy and the benefits of data sharing. This work describes the design process and an elicitation of preliminary requirements for a privacy dashboard that is developed in the context of the H2020 project HUMAN Manufacturing.

Keywords: Privacy · Dashboard · Smart manufacturing · Industry 4.0

1 Introduction

Smart manufacturing environments make use of data collected through smart sensor technologies (e.g., wearables, IoT) in the context of the Industry 4.0 paradigm [5,10]. Such technologies promise to increase productivity and support operators in their increasingly complex work as simple routine tasks are being automated. Much of the success of these new technologies depends on the availability of data related to the worker and the workplace. However, collecting data from and about workers in organisations is not a trivial task. Ensuring the safe, secure and correct use of the data by authorized people is one of the difficult challenges faced by many organisation in our increasingly data-centric world. Organisations need to build trust among their workers and trust in the organisation as well as making the services beneficial enough to convince workers

This research has received funding from the European Union's H2020 research and innovation programme under grant agreement no. 723737 (HUMAN).

Published by Springer Nature Switzerland AG 2020
I. O. Pappas et al. (Eds.): I3E 2019 Workshops, IFIP AICT 573, pp. 79–85, 2020.
https://doi.org/10.1007/978-3-030-39634-3_8

of the value in sharing their data. Consequently, a value and trust-based approach to data collection and use of data is necessary to achieve the purpose of facilitating trust between workers and their organisation.

This may require looking at trust and privacy from different perspectives, in particular, from the perspectives of the different stakeholders, when designing the various systems and technologies that are used by the workers. Privacy and trust in the workplace and in a working context not only require trust in a specific technology, but also in the organisation itself [2]. EU's General Data Protection Regulation (GDRP) [1] advocates privacy by design and privacy by default, which require considering privacy from the initial design stages and throughout the complete development process of new products, processes or services that involve gathering and processing personal data. It also means that when a system or service includes choices for the individual on how much personal data he or she shares with others, the default settings should be the most privacy friendly ones.

When considering productivity tools in the workplace, a particular tool that could be used to foster trust and accommodate regulatory pressure is a Privacy Dashboard[1], which put emphasis not only on the technological perspective (i.e., the ability to review/change one's own privacy), but also on the organisational and social perspectives. Privacy dashboards have been previously extensively researched, e.g. as a mechanism to enhance user control in the Privacy Bridges project [4], in the context of GDPR [9], or referred to as Privacy Mirrors in [7].

The main aim of this paper is to report our experience in designing a privacy dashboard for workers in the manufacturing industry, driven by the trust and privacy framework [6] developed within the context of the H2020 research project HUman MANufacturing[2]. The project researched the use of digital technologies (e.g., augmented reality and exoskeletons) to physically and cognitively enhance the workers on the shopfloor, which implied the use of wearable devices to collate information on the worker and their work context. Clearly, the gathering of personal data raises serious privacy concerns and hard challenges on workers' trust in both the digital solution and the organisation. So far, less attention has been paid to such an application area compared to the use of services in a private context (e.g. social networks).

The remainder of this paper is structured as follows. In the next Sect. 2, the smart manufacturing environment in HUMAN is described. In Sect. 3, we present the initial design process of the Privacy Dashboard and Sect. 4 concludes the paper.

2 Smart Manufacturing in HUMAN

The HUMAN project aims to digitally enhance the worker on the shopfloor to support them in their work, assisting them in mitigating any productivity losses resulting from either physical or cognitive fatigue whilst contributing to

[1] https://www.privacypatterns.org/patterns/Privacy-dashboard.

[2] http://humanmanufacturing.eu/.

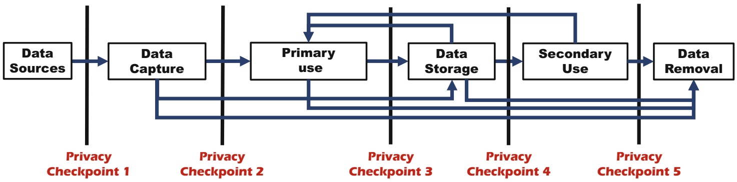

Fig. 1. Overview of data life-cycle transitions of the HTPF. Figure adapted from [6].

the worker's greater well-being. This is achieved by collating physiological data from the worker through wearable sensors and combining the production context (e.g. tasks, workplace) in which the worker is embedded. The primary use of the captured data is to reason, via different machine learning techniques, on how best to support the worker. However, the captured and processed data can also be re-used after being stored for analysis purposes, which may be an example for secondary use of the data. An example for such indirect usage is the improvement of workplaces or work processes by identifying bottlenecks in the production process when analysing aggregated historical data.

The underlying premise in HUMAN is to gather as much data as possible from the worker, their behavior and activities, to determine the best contextual support. However, this raises serious concerns over privacy and trust that may undermine the acceptance of the HUMAN system by the workers. As such, the HUMAN Trust and Privacy Framework (HTPF) was developed to support the dialogue amongst the different stakeholders in smart manufacturing work environments [6]. The HTPF (Fig. 1) is based on existing work on privacy in information systems (e.g. the design strategies in [3]) but puts emphasis on the lifecycle and transitions of data and a set of privacy checkpoints.

For each checkpoint, the HTPF provides guidelines for designers and developers of digital solutions to take the necessary precautions and actions for ensuring that the privacy of individuals and organisations are safeguarded, which will contribute to foster trust among the workers and within the organisation. The checkpoints serve as gateways, where the processing of the data may be different after that point. The main users of this framework will be designers and developers of IT systems and services and the individuals, groups or organisational units that will use and/or deploy these systems and services. From an end user's perspective, the HTPF illustrated in Fig. 1 can help to increase users' awareness about privacy and increase their knowledge of their rights to privacy and when and what they should expect of the services they use.

3 Design of the Privacy Dashboard

A key design principle adopted in the HUMAN project was the co-creation methodology, involving the different stakeholders from inception of ideas to the deployment of the prototypes for field evaluation. A strong requirement, driven by the users and supported by management, was the idea of a Privacy Dashboard

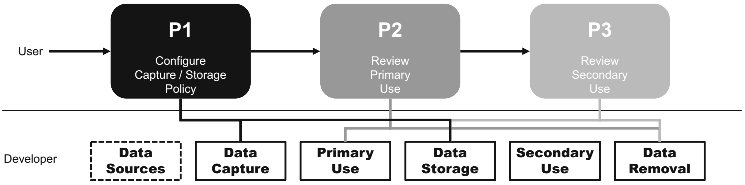

Fig. 2. Three main touch-points (P1-P3) with the Privacy Dashboard and their link to the HTPF.

that first emerged during a workshop on Opportunities and Threats with use case partners in a user study with the HUMAN consortium [8]. The potential threats related to organisations collecting significant amounts of personal data were clear, which would invalidate the potential benefits. The main reason for this was related to the potential risk of privacy violations and breach of trust. While they could appreciate the value of data collection and the potential benefits that could lead to, the representatives of the end-user organisations expressed the need for the workers to have control of their privacy settings and the need for transparency. Given these needs from the workers, and the requirement to be GDPR compliant, the idea of a privacy dashboard emerged. In the case of the HUMAN Knowledge In Time service, which uses AR to support the operator on the shop-floor, the aim of the Privacy Dashboard is to provide data owners, (e.g. workers), transparency about how their data is used as well as the option to limit the future usage of their data or delete previously stored data here and now.

3.1 Design Process

After the initial workshop, and aligned with the co-creation methodology, several workshops were conducted involving all the relevant stakeholders with privacy being a prominent feature continuously addressed in the development of the KIT service. The initial phase of the design was the identification and sketching of use cases, based on the analysis of the needs and requirements that emerged from the co-creation workshops conducted with the HUMAN consortium partners. Then, we used the HTPF to review each use case sketch based on the framework and its guidelines. Where relevant, we refined the existing use case sketches to ensure privacy by design, in the light of the framework; or defined new use case sketches to clarify and add detail to the original use cases.

The use of HTPF supported both the design of the dashboard and the dialogue with end-users. However, our studies within the HUMAN project show that the users found the framework useful in understanding their needs for privacy and consequences related to sharing their data. However, the user or worker is not likely interested in the subtle details of the privacy of the system, but rather in the privacy threat vs. benefits trade-off. Consequently, to facilitate the dialogue further with the users, the decision was made to simplify the HTPF for end users of the KIT solution, resulting in the diagram depicted in Fig. 2, where we identified three main touch-points through which workers would interact with the Privacy Dashboard. Nonetheless, each of the touch-points can be associated with one or more stages of the HTPF, which can help a developer in realising a concrete instance of the proposed dashboard. Each of the touch-points addresses one or more use cases of the privacy dashboard and, next to revealing already stored information or allowing to configure the applicable policies, also highlights the advantages as well as the threats of sharing one's personal data. In our preliminary analysis, we identified 9 use cases along with requirements for the Privacy Dashboard, which we group as follows to the three touch-points: Touch-point P1 (Configure Capture/Storage Policy) with use cases:

- Configure data capture policy (P1-1),
- Configure primary usage policy (P1-2),
- Configure data storage policy (P1-3),
- Configure secondary usage policy (P1-4), and
- Configure data removal policy (P1-5);

touch-point P2 (Review Primary Use) with use cases:

- Review/monitor data capture (P2-1) and
- Review/monitor primary data usage (P2-2);

and touch-point P3 (Review Secondary Use) with use cases:

- Review/monitor data storage (P3-1) and
- Review/monitor secondary data usage (P3-2).

As the design of the dashboard is ongoing, we envision that additional use cases may be identified. We now exemplify the envisioned design by describing functional requirements for two of the identified use cases.

Configure Data Capture Policy (P1-1). A primary use case of the touch-point P1 is to adjust the policy regarding the Data Capture phase of the life-cycle in the HTPF. From a developer's point of view, this policy corresponds to setting up what personal data may pass Privacy Checkpoint 2 in Fig. 1. From a user's perspective, the main question addressed by this use case is: *What do I want to share with only the system or other users of the system or the organisation?* We gathered the following requirements for the design from a user's perspective.

- Get information on why data needs to be captured.
- Configure what can be captured.
- Configure access rights to captured data (e.g., only the system or also other users).

Following this, there are the following requirements from a developer's perspective:

- Ensure user is informed of the implications of capturing data.
- Ensure user is informed of needs and benefits of capturing data.

In fact, from an organisations point of view the last requirement is essential when certain services can only be offered with access to the data. For example, when using the wearable sensors on the worker for activity recognition, then this can enable convenience services supporting the worker with just-in-time information. However, this could also be a privacy risk when being used for profiling an individual worker's performance.

Review/Monitor Secondary Data Usage (P3-2). The second use case that we want to highlight is related to touch-point P3. It is about reviewing how data was re-used for secondary purposes. Here, the main questions answered for the users is: *Who had access to the data capture/stored about me in the HUMAN system?* This corresponds to reviewing what data was transferred beyond Privacy Checkpoint 4 in Fig. 1 as well as to get insights on how it was used. Again, we gathered requirements from the user's perspective:

- Review who accessed my data and when;
- Review who could have accessed my data;
- Review for which purpose my data was accessed;
- Review which data was exported from the system;

and the developer's perspective:

- Provide transparency/notification of access rights and actual access;
- Provide transparency on the kind of use either based on individual features or application/services.
- Provide transparency on the outcomes, i.e., was it used for an intervention or caused changes in the work process.

Our goal for the design of the privacy dashboard is to put emphasis on providing transparency on the outcomes of the secondary data usage rather than just providing details on data usage which are difficult to interpret for users of the system.

4 Conclusion

This paper describes the design process and initial requirements identified in several use cases of a privacy dashboard to be used in a smart manufacturing environment. We used a recently proposed trust and privacy framework [6], which was developed in the same project, to guide the design process. We acknowledge that the design of the dashboard is at an early stage of requirements elicitation. In the future, we plan to implement a prototype and compare our design to existing privacy dashboards based on the specific requirements of work environments such as manufacturing plants.

References

1. European Union: Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation). Off. J. Eur. Union **L119**, 1–88 (2016)
2. Galford, R., Seibold Drapeau, A.: The enemies of trust. Harv. Bus. Rev. **81**, 88–95 (2003)
3. Hoepman, J.-H.: Privacy design strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T. (eds.) SEC 2014. IAICT, vol. 428, pp. 446–459. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55415-5_38
4. Irion, K., Yakovleva, S., Hoboken, J.V., Thompson, M.: A roadmap to enhancing user control via privacy dashboards. Tech. rep., IViR (2017)
5. Lasi, H., Fettke, P., Kemper, H.G., Feld, T., Hoffmann, M.: Industry 4.0. Bus. Inf. Syst. Eng. **6**(4), 239–242 (2014)
6. Mannhardt, F., Petersen, S.A., Oliveira, M.F.: A trust and privacy framework for smart manufacturing environments. J. Ambient Intell. Smart Environ. **11**(3), 201–219 (2019)
7. Nguyen, D.H., Mynatt, E.D.: Privacy mirrors: understanding and shaping socio-technical ubiquitous computing systems. Tech. rep., Georgia Institute of Technology (2002)
8. Petersen, S.A., Mannhardt, F., Oliveira, M., Torvatn, H.: A framework to navigate the privacy trade-offs for human-centred manufacturing. In: Camarinha-Matos, L.M., Afsarmanesh, H., Rezgui, Y. (eds.) PRO-VE 2018. IAICT, vol. 534, pp. 85–97. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99127-6_8
9. Raschke, P., Küpper, A., Drozd, O., Kirrane, S.: Designing a GDPR-compliant and usable privacy dashboard. In: Hansen, M., Kosta, E., Nai-Fovino, I., Fischer-Hübner, S. (eds.) Privacy and Identity 2017. IAICT, vol. 526, pp. 221–236. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-92925-5_14
10. Thoben, K.D., Wiesner, S., Wuest, T.: "Industrie 4.0" and smart manufacturing – a review of research issues and application examples. Int. J. Autom. Technol. **11**(1), 4–16 (2017)