In Our Employer We Trust: Mental Models of Office Workers' Privacy Perceptions*

Jan Tolsdorf[1 [0000−0002−1961−100X]] and Florian Dehling[1 [0000−0002−8824−2500]]

Data and Application Security Group
TH Köln - University of Applied Sciences, Cologne, Germany
https://das.th-koeln.de
{jan.tolsdorf, florian.dehling}@th-koeln.de

Abstract. The increasing digitization of the workplace poses new threats to the right to privacy for employees. Previous work on this matter was rather quantitative and with a strong focus on monitoring and surveillance. Yet, there is a lack of comprehensive explanations for employees' privacy perceptions and what drives their risk and trust perceptions.
We conducted an interview study with 22 German employees to qualitatively examine (1) issues and themes related to the expectations of privacy of office workers and (2) their beliefs and understandings of how their data is handled by their employers.
We present the mental model of the *believing employee*, which is characterized by a high level of trust in the lawful processing of personal data by the employer and little fear of invasions of privacy. The mental model is strongly influenced by the uncertainty regarding the processing of personal data by employers and compensates missing experiences regarding privacy at work with analogies from private online use.

Keywords: privacy in the workplace · privacy perceptions · informational self-determination · mental models

1 Introduction

The workplace undergoes major changes in times of digitization. In particular, it leads to an increase of companies processing personal data of their employees. Therewith associated threats to the preservation and assurance of the individual right to privacy have been disregarded lately. While employees demand for more transparency and control over their personal data [29], existing Privacy Enhancing Technologies (PETs) [32] and Transparency Enhancing Technologies (TETs) [25] are only available for the business-customer relationship. Their adoption to the working sphere is likely to fail when not fulfilling employees' mental models and actual privacy demands [14]. We contribute to this matter by presenting

* Supported by the German Federal Ministry of Education and Research (BMBF) under the research project "TrUSD - Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen" (transparent and self-determined design of data use in organizations).

Jan Tolsdorf, Florian Dehling, In Our Employer We Trust: Mental Models of Office Workers' Privacy Perceptions, Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2020 (FC). February 14, 2020 Kota Kinabalu, Sabah, Malaysia Springer, 2020

German office workers' mental models of privacy perceptions, in order to lay a basis for future tool developments. Our approach differs from that of a large stream of research that adapts the US-American definition of privacy as the *right to freedom from intrusion* [19]. Instead, we refer to a more holistic definition of privacy as the *right to informational self-determination* that warrants each individual transparency and personal control over the collection, use and disclosure of their personal data by others. This concept is very present in European and Canadian societies [19] and was also incorporated into the General Data Protection Regulation (GDPR) in the European Union. It has further paved the way for our modern understanding of information privacy, manifesting itself in the Privacy by Design (PbD) paradigm [12].

2 Related Work

Mental Models. Mental models (MMs) are simplified internal representations of external reality that enable individuals to make sense of their environment, including simple actions, systems or even complex phenomena [18]. MMs are generally considered to be incomplete [27], incorrect and highly context-dependent, making them unstable or rather inconsistent. Irrespective of their correctness towards representing a phenomena, MMs are incredibly helpful in given or unfamiliar situations by guiding the decision making process to behave in a certain way [10]. In the context of HCI and privacy, previous work has primarily considered MMs of privacy in general [28] and in the context of private technology use [14, 15]. The latter with a strong reference to online services [7, 20, 30, 31]. Individuals were found to rely on several incomplete and poorly formed submodels [30] or use highly simplified models, even against better knowledge [2].

Privacy Perceptions in the Workplace. Information privacy in the work context was found to be (at least) a tripartite concept comprising of employees' beliefs in having control over the (1) gathering (e.g. collection and storage) and (2) handling (e.g. processing) of personal information as well as the (3) perceived legitimacy of the employer to process data (e.g. expected usage) [3, 9].

Investigations on privacy perceptions in the workplace are strongly marked by theoretical considerations or empirical findings of quantitative studies based on "privacy as intrusion" [34, 35, 37] and the overall topic of employee monitoring and workplace surveillance [4]. While many employees agree that it is mostly used for coercive control reasons instead of caring reasons, only few employees reported it to be an invasion of their privacy [36]. Besides, employees are aware that disclosure of certain personal information is unavoidable in the course of their employment and are aware of possible privacy invasions [5]. Though, they may deliberately withhold data if they expect benefits [5] or fear adverse consequences [33]. Employees were also found to weigh up constraints over affordances [23], substantiating the validity of the privacy calculus [11] in the workplace: employees are generally willing to disclose information if they receive adequate gratification in return. High levels of concern and anxiety regarding the misuse of information by the employer are reasons that hinder disclosure.

3 Methodology

To elicit MMs of employees' privacy perceptions in digitized workplaces, we conducted semi-structured interviews with 22 employees from small to large sized organizations in Germany during the period July until September 2019.

Participants and Recruiting. We aimed at recruiting a heterogeneous sample in terms of people with different professional and socio-demographic backgrounds in order not to limit privacy perceptions by demographic characteristics [21]. Participants were invited using organizations' internal mailing lists or direct invitation. Employees participated voluntarily and without payment, though some employees were exempted from normal duties for participation during working hours. Participants' demographics are available in Appendix A.

Interview Guideline Design. We adopted an *expert model* approach to design an appropriated interview guideline, as it proved itself valuable in eliciting mental models before [7, 24]. We executed an iterative development process: we derived an initial version of the expert model by capturing and sorting all relevant aspects from selected themes on data protection law, general privacy literature, as well as technical and organizational circumstances of workplace environments. The model was then repeatedly reviewed and discussed in expert groups, with participants from the various fields of law, psychology, ergonomics, IT systems engineering, security and privacy, followed by subsequent adjustments of the model. We further conducted three pilot interviews to check the validity of the interview guideline's questions and structure. A copy is available in Appendix B.

Evaluation. We conducted a qualitative analysis by carrying out a deductive coding approach by converting the expert model to a code-book. We followed established guidelines [22] and common practices for semi-structured interviews [8]. First, transcribed audio recordings were segmented into thematic sections based on our interview guideline. Then, a randomly selected 50%-subset of the interviews was independently coded by two researchers. In a subsequent revision step, a *negotiated agreement* approach was used to discuss disagreements and resolve coding differences by revising the categories and coding scheme in order to avoid interpretation bias. Afterwards, the same two coders coded all interviews. Gwet's gamma (AC2) [16] was used as a measure of the quality of the inter-rater agreement (IRA) as it takes into account the kappa-paradox, a problem where low kappas occur despite a high percentage of agreement [13].

Limitations. As participation was voluntary, sampling is affected by self-selection bias and limited to the population of people being employed at the organizations we contacted. Despite individual demographic differences, our sample contains only participants with a German cultural background. The results might not be the same in different cultures or organizations. Since a qualitative approach was chosen, we do not claim to provide generalization on the topic of employee privacy perceptions, but aim at elaborating and exploring reasoning and views.

Ethics. Our study complies with the strict German and European privacy regulations. The data was either collected anonymously or converted to anonymous data after the interview. Any contact information was stored separately. Participants were informed about their right to withdraw their data during or after the study. We emphasized that leaving the interview will not have any negative consequences and assured that neither the fact of their participation nor the interview's content will be reported back to their employer.

4 Findings

In the following section, we present our findings based on our coding. Only codes with at least moderate agreement ($IRA_{AC2} > 0.74$) are respected.

4.1 Self-Disclosure & Consent

We asked interviewees about their abilities and liberties to take control over data disclosure and how they agreed to its use by the employer.

Employees as Data Providers. The vast majority of participants responded that they actively disclose data to their employers *"systematically within the scope of data entry forms"*. Participants were particularly conscious about the data they provided during the recruitment process. Participant P06 noted that disclosure then rather happens in the course of *"personal conversation or even written exchange"*. In this regard, one participant indicated that it is generally hard to tell who had access to documents (i.e. CV) and is in possession of what kind of information. Participant P14 did not consider his employer to *"actively obtain data from me, instead I rather believe that I provide data"* and compared himself to a kind of data provider who is in control over what data will be disclosed. Another employee commented *"I have no qualms in that case. If I believe that my employer is allowed to be interested in gathering my data and that's what he needs, he gets the data - anything else that goes beyond that, I refuse."* Two senior executives claimed to even have some control over the use of disclosed data. While one of them manifested his control beliefs by being responsible for performing certain data processing operations, the other linked the freedom and ability to actively input data into systems he has access to as control capabilities.

Concern. We found that employees reported to be generally unconcerned when disclosing personal information, justifying their attitudes with strong trust beliefs. Participant P06 expressed that *"in the course of digitization and Facebook and no idea what else there is [...] I can already imagine that more can happen with the data [...] But I would say that my employer doesn't do that"*. In line with this view, various participants justified their lack of concern by referring to law, claiming that their employer *"will of course adhere to the applicable data protection regulations"* as *"this is top priority"* to the organization and its employees. A manager put emphasis on the appropriateness of the types of data

that is elicited: *"employers do not record eye color, nose length or shoe size, but record the data necessary for the contractual relationship and payroll accounting"*, concluding that there is no reason to be concerned or worried about. Only one participant showed concerns and directed attention to a loss of control and uncertainty going along with the disclosure of sensible personal data to employers: *"in the worst case, it could even be used against me at some point."*

Giving Consent. When being asked how they agreed to the use of their data by their employer, participant P08 responded: *"Not at all. Or simply by providing it - it was tacit consent."* The majority of respondents gave similar explanations and characterized their consent therefore as *implicit*. Participant P16 explained that the consent *"is not stated in my employment contract, [instead] this is done here on a basis of trust"*. Participants emphasized that implicit consent is not necessarily a loss of control. Instead, active data disclosure was seen as a form of *"indirect approval"* because one is *"still conscious of [disclosing] it"*. However, there were also participants who admitted not to *"remember if there was a consent form back then"* (P05). In such cases, employees stated that they really do not mind their data being processed anyway.

Half of the participants declared that they *explicitly consent* and claimed to have actually signed a corresponding data protection statement at the beginning of their employment which is ultimately valid. Moreover, implicit and explicit consent are by no means dichotomous, but the type of consent *"depends on the type of data, [...] for many [data] there do exist privacy declarations stating that the data can be used"* (P11) and that one usually signs at the beginning of an employment. Consent for subsequent data disclosures, however, occurs implicitly: *"but then there is also a lot of data, which is naturally produced as you work. Which means, of course, that there is no need for separate approval"*.

4.2 Data Processors.

When we asked who collects and processes personal information in the course of their professional activities, all except one participant mentioned entities both inside and outside their respective organizations. The one who disagreed claimed that her personal data is *"certainly not!"* processed nor collected by external entities outside her organization because she is *"very, very careful"*.

Legally Mandatory Entities. Two-thirds of the respondents named external data processors who are legally mandatory for an employment relationship. Thereby, registration with the social security agency at the beginning of the employment and paying income tax to the tax authority were most frequently mentioned, followed by health insurance companies and the statutory pension insurance.

Service Providers & Customers. Regardless of employer or occupation, employees named service providers, customers and business partners as external data processors who receive and process at least partial extracts of their personal data. Yet there was a tendency to not know what kind of information this involves. For

example, while one employee assumed that data is shared anonymously, the senior manager clearly stated that the data *"contains the first name and surname and the professional e-mail address"*. Similarly, other participants reported they are unaware of the exact data but expect their employer to abide the law, act most carefully and to only share little information.

Human Processors. Our results suggest that office workers think of human-like data processors, since any processing was associated with some form of human interaction. We did not find any evidence for autonomous or purely algorithmic processing being part of the participants' explanations. Unlike participants from medium and large organizations, employees from the small sized enterprise generally only referred to a specific person when explaining business processes and giving examples. They were also very aware of the fact which person has access to what kind of data. While employees were generally familiar with information systems at the workplace, they only attributed data storage purposes to it.

Communication & Internet Services. Solely participants with an IT background mentioned communication service providers and intermediary systems when being asked about external processors. Participant P10 pointed out that there are no differences between private and work related internet use as *"every moment you are on the internet data is collected"*. In this context, participant P21 noted that popular service providers *"now also know that I work here"* as he uses his private accounts for work as well. A senior employee showed awareness of the fact that he possesses an account for the manufacturer of their business software, but added *"I'm actually not sure what data [the manufacturer] has about me, ... there is obviously somehow also an account which was set up there for me, so probably data also flowed, but I don't know which data"*. Participant P04 explained that with modern software it is difficult to know whether and if so which data the manufacturers may collect *"unintentionally"* and explained that *"there is also a lack of transparency for the most part - even if you choose that no data should be sent"* it might still happen. For instant messaging apps and email, participant P14 also claimed that *"providers get at least the message and then my name, they know where I work"*. Participant P12 pointed out that even the simplest processes involve several different and often unknown intermediaries.

4.3 Purposes of Data Processing.

We asked about the purposes for which their employers process personal data. Respondents broadly agreed that the data would be processed primarily in the context of normal employment processes and considered it as justified and fully legitimate, although it may leads to very undesirable consequences for employees.

Administration Tasks. The overwhelming majority of participants agreed that their data would be used primarily "*for all correspondence and salary payments"*. Certain data were thereby assigned to specific purposes. For example, participant P04 explained that *"the bank account is used for the salary transfer, the date*

of birth to register me at the competent authority, my social security number because of the salary". Though, further purposes other than administration tasks were mentioned; an employee from the public sector explained that her employer requires certain personal information related to skills and education in order to determine *"what to do with [her]"* and assign her suitable activities.

Acquisition. Employees from the private sector replied that their employers disclose information on their skills to potential customers to acquire new orders. Participant P16 stated: *"[my employer uses it] for economic purposes - to sell me!"*. Another employee pointed out that this kind of personal information is *"also data I publish privately on [an employment-oriented social networking site]"* and therefore, the data that his employer discloses to potential customers is *"publicly available anyway"*. Yet, he remarks that *"some of my colleagues may not have done that - in this regard it is only okay for me personally"*.

Employee Assessment. Participants from the private sector discussed the topic of employee assessment, considering *performance evaluation* and *suitability determination*. Evaluation could either have positive or negative results for the respective employee. Yet, negative consequences were not linked to their own employment, but to hypothetical scenarios with either other or fictitious employers. Participant P08 summarized these topics stating that he can *"well imagine that some employers collect information about their employees to be able to get rid of them if necessary, or when it comes to announcing dismissals, in order to be able to react accordingly, or when salary demands or additional requests come in, to have something available to compare employees. When it comes to promotion to know who is best suited or is not well suited, i.e. is not able to work under pressure, is often ill, is irascible, has any convictions which stand in the way of promotion"*. Monitoring activities such as working time tracking were also particularly present in this context.

Duty of Care. However, working time tracking was not exclusively linked to employee surveillance activities. In fact, a small group of participants noticed that employers have a duty of care to their employees and considered this as a valid and important purpose to process individual-related data. Most present was the issue of overworking and inadequate rest or vacation periods in this context. A team manager elaborated on this topic and referred to situations where employees carry out various activities alongside their job. He explained that for employees in his team, he expects them to disclose certain information about their private lives in order for him to both, verify that employees meet their obligations and secondly, in order to fulfill his duty of care.

4.4 Invasion of Privacy.

To better understand employees' perceptions of privacy violations, we asked participants to discuss aspects and situations that would violate their privacy.

Data usage without knowledge. We asked participants about their thoughts and judgment on their data being processed without their knowledge - two distinct positions emerged: Some of the subjects stated that they would perceive such processing as a restriction of their privacy. They considered the linkage of working times and ticket systems or the interpretation of financial and health data. For example, participant P15 expressed concerns about the handling of sick notes that must be sent to the employer, but may contain hidden clues about the illness. She justified her uneasiness with the resulting uncertainty as to what conclusions would be drawn from it: *"then it goes on to the headquarters and then you just don't know what conclusions they draw from it"*.

Contrary, a much larger group of participants did not express any concern with unwitting use. They either doubted the need to be notified about the forwarding: *"I'm gonna say no, otherwise [the employer] would have done it."* (P20); emphasized its legitimacy: *"I think if the data is used then I already assume that this is appropriate"* (P14); or pointed out that they *"don't have any big problems with that, they are also no particularly precarious data"*.

Ways of abusive data usage. We asked participants for what purposes their employer may use their data and also asked for practical examples of data misuse. Thereby, interviewees raised concerns about the transfer of their data to third parties - two models got identified in this thematic area: one describes the sale of employee data with vague intentions. Participant P03 claimed that an illegal usage of data has to be bound to a somehow *"commercial interest"*. Even more prevalent was the idea of employers passing on personal data to advertisers: *"the employer could also pass the data on to companies that collect e-mail addresses, postal addresses, for advertising, for calls, for any subscription sales, surveys, etc."* (P08). The second model identified is closer related to the work environment and aims at targeted advertisements based on data which gets transmitted to insurance providers by employers: *"I know that health insurance policies for privately insured persons or civil servants are always opened at the right time in order to obtain their deals"* (P01). One participant thought of an even more explicit use of advertisement in the workplace, describing that employers could be *"passing on data to advertising agencies in order to place targeted advertisements to enforce certain behavior at work the employer benefits from."*

5 Discussion

Contrary to our expectations, we generally did not identify groups based on participants' demographic backgrounds that can be linked to a particular set of attributes on privacy beliefs and perceptions. Instead we identified recurring statements and justifications among all of our participants. We refer tho this overarching mental model as *the believing employee:* First of all, our participants were largely satisfied with the ways in which they regulated disclosure and how they disclosed the data. Almost all participants uttered to at least partially give implicit consent to data processing and considered it as sufficient for

disclosure in daily business. Also, participants hardly expressed concerns and demonstrated to have strong trust beliefs in the lawful processing by employers. Yet, respondents were often unaware of what data was actually available to their employer or third parties, even though they themselves claimed to have actively provided it. This applies to both data made available during the application process and also to data from the normal working routine. Still, all subjects showed awareness for their employers' reasons behind the processing and disclosure of certain personal data. This finding entails that employees assumably possess a certain baseline set of associations between actual data and purposes and thus only require additional support in cases of unexpected data usage or data flows. Concerning abusive data usage, the kind of possible misuse scenarios that our participants expressed indicate that they made use of analogies from their private lives. The majority of participants stated that their data could be misused for advertising purposes. Some respondents made comparisons with services such as Facebook or Google, which indicates that they mapped the risks and consequences they experienced in their private sphere to the work context.

Apart from these commonalities in the vast majority of the participants' answers, we also found nuances in the consideration of *knowledge* and *uncertainty*; considering *knowledge*, participants' explanations were naturally biased by additional knowledge they possessed either due to their position or their profession. That is, managers superior knowledge on data flows influenced their beliefs on control. Similarly, only IT professionals identified intermediary services as hidden data processors, whereas non-IT professionals were particularly ignorant about these entities. We refer to this nuanced model as *the knowing & informed employee*; with regards to *uncertainty*, we found that some participants expressed concern due to a lack of transparency about which data were available to their employers. In particular, permanent data storage is regarded as a threat because employers are believed to be able to use it against workers at any time. Similar to previous findings [5, 33], these participants perceived unwitting processing of personal data as a violation if they feared negative effects for their careers. We refer to this theme as *the fearing employee*.

5.1 Implications for Transparency and Control

From our findings we deduce that transparency rather than control over personal data is required by office workers. There are two reasons for this: first, employees are seemingly happy with the control abilities they currently have; second, the overall high level of uncertainty holds risks for employees' privacy at work as it is known to lead to adverse effects and paradoxical observations [1]. The general lack of knowledge about who has access to personal data stands in contradiction to the fundamentals of informational self-determination. In this regard, *privacy dashboards* have proven themselves useful in improving awareness and transparency of users in online services [6, 38] and are currently reviewed in the scope of organizations as well [29]. But also the implementation of *privacy notifications* in the workplace have the potential to contribute to more awareness. While this measure is known to be effective for making informed privacy decisions [17, 26],

its implementation is often challenging to not annoy users. However, our results indicate that their use can well be limited to certain processes. The use of analogies from private lives for data misuse scenarios demonstrates that the complexity of the subject exceeded the cognitive abilities of our participants. We assume that they have not been confronted with data abuse by employers before. However, a clear understanding of risks is indispensable to make informed privacy decisions. Further research is needed to raise awareness in this topic without unnecessarily burdening the relationship between employee and employer.

6 Conclusion

Our findings show that privacy perceptions at work are largely uniform among employees of different professions and organizations. We identified three mental models of privacy perceptions with tiny but distinct differences:

(1) The *believing employee* is characterized by a very high level of faith in employers to comply with legal requirements when processing personal data and is heavily influenced by an uncertainty bias which compensates for missing factual knowledge. They are aware aware of active data disclosure and are thus comfortable with using implicit consent by either disclosing or withholding data. Unwitting data usage does not constitute a violation of privacy while unlawful data processing is attributed exclusively to other employers. Any violations of privacy are heavily primed by the use of analogies from the private sphere.

(2) The *knowing & informed employee* represents a nuance of the *believing employee* that justifies in additional knowledge on a topic on data processing activities in the organization. Knowledge may come from the position in the company or the professional background. The employee falls back into the believing model in situations where additional information is unavailable.

(3) The *fearing employee* also represents a nuance of the *believing employee*, which is reflected in the fact that uncertainty is expressed in concern about possible negative consequences of employers data processing. Ignorance of what information employers have available contributes to a high degree of uncertainty in the disclosure of data. Unwitting data usage that results in unintended consequences for employees is perceived an invasion of privacy.

The main challenges for the future are to close gaps and deal with misunderstandings regarding the access of individuals and organizations to employees' personal data, and to provide transparency on data processing so that employees can act in a self-determined manner and not under uncertainty and belief.

Acknowledgments

The authors would like to thank Hartmut Schmitt and Svenja Polst for their support in conducting interviews, the involved organizations for their support in recruiting participants and last but not least all employees for their participation and valuable insights on privacy perceptions in the workplace.

Bibliography

[1] Acquisti, A., Brandimarte, L., Loewenstein, G.: Privacy and Human Behavior in the Age of Information. Science **347**(6221), 509–514 (2015), https://doi.org/10.1126/science.aaa1465

[2] Acquisti, A., Grossklags, J.: Privacy and rationality in individual decision making. IEEE Security and Privacy Magazine **3**(1), 26–33 (2005), https://doi.org/10.1109/MSP.2005.22

[3] Alge, B.J., Ballinger, G.A., Tangirala, S., Oakley, J.L.: Information Privacy in Organizations: Empowering Creative and Extrarole Performance. Journal of Applied Psychology **91**(1), 221–232 (2006), https://doi.org/10.1037/0021-9010.91.1.221

[4] Backhaus, N.: Context Sensitive Technologies and Electronic Employee Monitoring: a Meta-Analytic Review. In: 2019 IEEE/SICE International Symposium on System Integration (SII), pp. 548–553 (2019), https://doi.org/10.1109/SII.2019.8700354

[5] Ball, K., Daniel, E.M., Stride, C.: Dimensions of employee privacy: an empirical study. Information Technology & People **25**(4), 376–394 (2012), https://doi.org/10.1108/09593841211278785

[6] Buchmann, J., Nebel, M., Roßnagel, A., Shirazi, F., Simo, H., Waidner, M.: Personal Information Dashboard: Putting the Individual Back in Control. In: Hildebrandt, M., O'Hara, K., Waidner, M. (eds.) Digital Enlightenment Yearbook 2013, pp. 139–164, Iso Press, Amsterdam, Netherlands (2013)

[7] Camp, L.J.: Mental models of privacy and security. IEEE Technology and Society Magazine **28**(3), 37–46 (2009), https://doi.org/10.1109/MTS.2009.934142

[8] Campbell, J.L., Quincy, C., Osserman, J., Pedersen, O.K.: Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. Sociological Methods & Research **42**(3), 294–320 (2013), https://doi.org/10.1177/0049124113500475

[9] Chen, X., Ma, J., Jin, J., Fosh, P.: Information privacy, gender differences, and intrinsic motivation in the workplace. International Journal of Information Management **33**(6), 917–926 (2013), https://doi.org/10.1016/j.ijinfomgt.2013.08.010

[10] Craik, K.J.W.: The Nature of Explanation. Cambridge: Cambridge University Press (1943)

[11] Dinev, T., Hart, P.: An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research **17**(1), 61–80 (2006), https://doi.org/10.1287/isre.1060.0080

[12] Domingo-Ferrer, J., Hansen, M., Hoepman, J.H., Le Métayer, D., Tirtea, R., Schiffner, S., Danezis, G., European Union, European Network and Information Security Agency: Privacy and data protection by design - from policy to engineering. ENISA, Heraklion (2014)

[13] Feinstein, A.R., Cicchetti, D.V.: High agreement but low Kappa: I. the problems of two paradoxes. Journal of Clinical Epidemiology **43**(6), 543–549 (1990), https://doi.org/10.1016/0895-4356(90)90158-L

[14] Fischer-Hübner, S., Pettersson, J.S., Angulo, J.: HCI Requirements for Transparency and Accountability Tools for Cloud Service Chains. In: Felici, M., Fernández-Gago, C. (eds.) Accountability and Security in the Cloud: First Summer School, Cloud Accountability Project, A4Cloud, Malaga, Spain, June 2-6, 2014, Revised Selected Papers and Lectures, pp. 81–113, Lecture Notes in Computer Science, Springer International Publishing, Cham (2015), https://doi.org/10.1007/978-3-319-17199-9_4

[15] Gerber, N., Zimmermann, V., Volkamer, M.: Why Johnny Fails to Protect his Privacy. In: 2019 IEEE European Symposium on Security and Privacy Workshops (EuroSPW), pp. 109–118 (2019), https://doi.org/10.1109/EuroSPW.2019.00019

[16] Gwet, K.L.: Computing inter-rater reliability and its variance in the presence of high agreement. British Journal of Mathematical and Statistical Psychology **61**(1), 29–48 (2008), https://doi.org/10.1348/000711006X126600

[17] Jackson, C.B., Wang, Y.: Addressing The Privacy Paradox Through Personalized Privacy Notifications. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. **2**(2), 68:1–68:25 (2018), https://doi.org/10.1145/3214271

[18] Jones, N., Ross, H., Lynam, T., Perez, P., Leitch, A.: Mental Models: An Interdisciplinary Synthesis of Theory and Methods. Ecology and Society **16**(1) (2011), https://doi.org/10.5751/ES-03802-160146

[19] Krebs, D., Doctor, J.: "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law? JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law **4**(1), 2 – 20 (2013)

[20] Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L., Vitak, J.: 'No Telling Passcodes Out Because They'Re Private': Understanding Children's Mental Models of Privacy and Security Online. Proc. ACM Hum.-Comput. Interact. **1**(CSCW), 64:1–64:21 (2017), https://doi.org/10.1145/3134699

[21] Kwasny, M., Caine, K., Rogers, W.A., Fisk, A.D.: Privacy and Technology: Folk Definitions and Perspectives. Technical HFA-TR-0804, Atlanta, GA: Georgia Institute of Technology School of Psychology – Human Factors and Aging Laboratory, Florence, Italy (2008)

[22] Mayring, P.: Qualitative Content Analysis [28 paragraphs]. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research **1**(2), Art. 20 (2000), https://doi.org/10.17169/fqs-1.2.1089

[23] Mettler, T., Wulf, J.: Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective. Information Systems Journal **29**(1), 245–273 (2019), https://doi.org/10.1111/isj.12205

[24] Morgan, M.G., Fischhoff, B., Bostrom, A., Atman, C.J. (eds.): Risk communication: a mental models approach. Cambridge University Press, Cambridge, New York (2002)

[25] Murmann, P., Fischer-Hübner, S.: Tools for Achieving Usable Ex Post Transparency: A Survey. IEEE Access **5**, 22965–22991 (2017), https://doi.org/10.1109/ACCESS.2017.2765539

[26] Murmann, P., Reinhardt, D., Fischer-Hübner, S.: To Be, or Not to Be Notified: Eliciting Privacy Notification Preferences for Online mHealth Services. In: In Proceedings of the 34th IFIP International Information Security and Privacy Conference (IFIP SEC), Lisbon, Portugal (2019)
[27] Norman, D.A.: Some observations on mental models. In: Gentner, D., Stevens, A.L. (eds.) Mental Models, pp. 7–14, Lawrence Erlbaum Associates Inc. (1983)
[28] Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Balebako, R., Cranor, L.F.: Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. Proceedings on Privacy Enhancing Technologies **2018**(4), 5–32 (2018), https://doi.org/10.1515/popets-2018-0029
[29] Polst, S., Kelbert, P., Feth, D.: Company Privacy Dashboards: Employee Needs and Requirements. In: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, Orlando, FL, USA (2019)
[30] Prettyman, S.S., Furman, S., Theofanos, M., Stanton, B.: Privacy and Security in the Brave New World: The Use of Multiple Mental Models. In: Tryfonas, T., Askoxylakis, I. (eds.) Human Aspects of Information Security, Privacy, and Trust, pp. 260–270, Lecture Notes in Computer Science, Springer International Publishing (2015)
[31] Schomakers, E.M., Lidynia, C., Ziefle, M.: Hidden within a Group of People - Mental Models of Privacy Protection:. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security, pp. 85–94, SCITEPRESS - Science and Technology Publications, Funchal, Madeira, Portugal (2018), https://doi.org/10.5220/0006678700850094
[32] Shen, Y., Pearson, S.: Privacy Enhancing Technologies: A Review. Technical HPL-2011-113, HP Laboratories, UK (2011)
[33] Smith, S.A., Brunner, S.R.: To Reveal or Conceal: Using Communication Privacy Management Theory to Understand Disclosures in the Workplace. Management Communication Quarterly **31**(3), 429–446 (2017), https://doi.org/10.1177/0893318917692896
[34] Stone, E.F., Gueutal, H.G., Gardner, D.G., McClure, S.: A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology **68**(3), 459–468 (1983), https://doi.org/10.1037/0021-9010.68.3.459
[35] Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W., Fromkin, H.L.: Employee perceptions of invasion of privacy: A field simulation experiment. Journal of Applied Psychology **66**(3), 308–313 (1981), https://doi.org/10.1037/0021-9010.66.3.308
[36] Watkins Allen, M., Coopman, S.J., Hart, J.L., Walker, K.L.: Workplace Surveillance and Managing Privacy Boundaries. Management Communication Quarterly **21**(2), 172–200 (2007), https://doi.org/10.1177/0893318907306033
[37] Woodman, R.W., Ganster, D.C., Adams, J., McCuddy, M.K., Tolchinsky, P.D., Fromkin, H.: A Survey of Employee Perceptions of Information Pri-

vacy in Organizations. Academy of Management Journal **25**(3), 647–663 (1982), https://doi.org/10.5465/256087

[38] Zimmermann, C., Accorsi, R., Müller, G.: Privacy Dashboards: Reconciling Data-Driven Business Models and Privacy. In: 2014 Ninth International Conference on Availability, Reliability and Security, pp. 152–157 (2014), https://doi.org/10.1109/ARES.2014.27

Appendix A Participants

Table 1. Participants Demographics

ID	Age	Sex	Education	Employment (years)		Profession	Organization Size
				Total	Current Employer		
P01	46-55	m	academic degree	21-25	6-10	Administration Employee	L
P02	56-65	f	academic degree	26-30	0-5	Administration Employee	L
P03	46-55	m	academic degree	16-20	6-10	Administration Employee	L
P04	26-35	m	apprenticeship	6-10	0-5	Software Developer	M
P05	46-55	f	higher education entrance qualification	26-30	6-10	Administration Employee	L
P06	46-55	f	secondary school or higher	31-35	31-35	Administration Employee	L
P07	36-45	m	higher education entrance qualification	21-25	11-15	IT Administrator	S
P08	46-55	f	apprenticeship	31-35	11-15	Sales	S
P09	46-55	m	apprenticeship	36-40	11-15	Supporter	S
P10	26-35	m	apprenticeship	6-10	0-5	Software Developer	S
P11	46-55	m	academic degree	21-25	6-10	Administration Employee	L
P12	36-45	m	academic degree	11-15	6-10	Research Assistant IT	L
P13	26-35	f	academic degree	11-15	11-15	Software Developer	M
P14	26-35	m	academic degree	6-10	6-10	Software Developer	M
P15	36-45	f	academic degree	16-20	11-15	Research Assistant IT	L
P16	18-25	m	academic degree	0-5	0-5	Software Developer	M
P17	56-65	f	academic degree	26-30	0-5	Administration Employee	L
P18	46-55	m	academic degree	16-20	0-5	Software Developer	M
P19	46-55	m	academic degree	16-20	6-10	Administration Employee	L
P20	44-45	f	academic degree	21-25	11-15	Software Developer	M
P21	18-25	m	academic degree	0-5	0-5	Research Assistant IT	L
P22	26-35	f	secondary school or higher	16-20	16-20	Administration Employee	L

Appendix B Interview Outline (Translated)

1. Welcome and general instructions: At the start of the interview, participants were welcomed and briefed about the study procedure, the study conditions and asked for their consent to elicit data (drawings, hand writings, answers to questionnaire, voice recording).
2. Use of technical tools during everyday work: In the first part of each interview, participants were asked to summarize their job profile and to explain the kind of technical tools (hardware and software) they use for their ordinary working activities. All tools were written down on moderation cards and displayed on the table.

   - Please describe to me with which tasks you mainly deal with in your daily work.
   - Which technical aids or tools do you use in your daily work?
3. Data gathering and processing by employers: The next part of the interview consisted of questions related to how employers gather data from their employees, for what purposes employees believe their employers require and process data about them and on employers' abilities and liberties to take control over data disclosure. We further elaborated on these topics by asking whether third parties are involved in any of these activities and asked them to draw or rather sketch data flows if they answered yes.
   - How does your employer obtain such data from and about you?
   - For what purposes can this data be used?
   - How do you consent to the use of this data?
   - What freedoms do you have when it comes to your company data?
   - Are there any third parties besides your employer who use or collect such data about you within the scope of your activities?
4. Privacy expectations: We asked participants about their awareness of data processing and possible data misuse scenarios.
   - Do you think it is possible for your employer to use data about you without your knowledge?
   - Suppose an employer collects or uses data without the consent of its employees: What consequences could data misuse have for employees?
5. Debriefing and questionnaire on demographics: At the end of the survey, participants were asked whether they want to add anything to the previous discussion and to fill out a post-questionnaire on demographics.