Privacy ad Absurdum

How Workplace Privacy Dashboards Compromise Privacy

Svenja Polst
svenja.polst@iese.fraunhofer.de
Fraunhofer IESE
Kaiserslautern, Germany

Denis Feth
denis.feth@iese.fraunhofer.de
Fraunhofer IESE
Kaiserslautern, Germany

ABSTRACT

In times of data-driven business, privacy and data protection are gaining importance. Users and legal bodies require the implementation of privacy-enhancing and transparency-enhancing technologies, such as privacy dashboards. Even though privacy dashboards contribute to privacy and data protection, they may also carry risks themselves. For example, privacy dashboards require access to and collection of quite a huge amount of personal data. This of course leads to a conflict with their primary goal—namely privacy, including data-minimization—and thus leads it ad absurdum. We particularly focus on privacy dashboards for employees as an example technology for transparency and self-determination at their workplace. Conflicts address among others transparency vs. data-minimization, and self-determination vs. social pressure. In this paper, we elaborate such conflicts and discuss corresponding solution strategies.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; **Usability in security and privacy**; • **Human-centered computing → HCI design and evaluation methods**.

KEYWORDS

Usable Privacy, Conflicts, Software Quality, Privacy Paradox

1 INTRODUCTION

With the rise of digital technology, companies are increasingly processing personal data (e.g., of customers, employees, partners) to offer their services. Thus, the management of personal data is an integral part of companies' daily business. Requirements for the management of personal data are given by legal bodies, for example, the European General Data Protection Regulation (EU-GDPR) [5]. Such regulations aim at protecting the data subject's (any person whose personal data is being collected, held or processed) privacy by ensuring transparency and self-determination. Companies can implement these requirements with appropriate privacy-enhancing technologies (PETs) and transparency-enhancing technologies (TETs), such as privacy dashboards, privacy policies, or anonymization procedures. In this paper, we focus on privacy dashboards and particularly elaborate on workplace privacy dashboards, i.e., privacy dashboards for employees, who are the data subject.

1.1 Problem & Contribution

During the conception of workplace privacy dashboards in our project "TrUSD"[1], also negative implications and concerns with respect to privacy dashboards arose. More specifically, the introduction of privacy dashboards poses problems that should be solved by them. We faced the issues that transparency might contradict data-minimization and might open the door for surveillance, self-determination can lead to social pressure, the centrality of privacy dashboards eases attacks, and trust might actually be decreased by the dashboard. In this position paper, we discuss use cases for privacy dashboards, their positive contribution to privacy, contrast them with the upper-mentioned conflicts aspects, and discuss possible solution strategies. The conflicts we discuss are based on the requirements we elicited in our project, and considerations of the project team, which has expertise in the fields of software engineering, usable privacy and legal regulations. The list of conflicts is thus not complete and solution strategies are not fully generalizable. However, by incorporating conflicts and solution strategies into corresponding quality models, quality standards and pattern collections, we hope to improve the quality of privacy dashboards.

1.2 Paper Structure

In section 2, we present related work in the areas of usable privacy, quality models and conflicts. In section 3, we explain what use cases a privacy dashboard should ideally offer, based on the state of the practice, the legal and the data subject's perspective. With this as a background, we present and discuss the mentioned arising conflicts in section 4. We conclude in section 5 and discuss future work.

2 RELATED WORK

In the following, we discuss related work regarding usable security & privacy, and quality models & quality conflicts.

2.1 Usable Security and Privacy

Privacy dashboards are our measure of choice to increase privacy. In general, various projects evaluate the applicability and usability of privacy dashboards. In the myneData project [17], for example, a user-controlled data market for personal data is being created. A decentralized solution is the MyData project [19], in which a cockpit is only used for transparency and control, but data remain with the services and can be exchanged via (existing) channels after

[1] https://www.trusd-projekt.de

MuC'20 Workshops, Magdeburg, Deutschland

https://doi.org/10.18420/muc2020-ws119-004

user consent. In the SPECIAL project [14], a holistic approach is being developed, in which data from various sources is aggregated and harmonized on the basis of machine learning and semantic technologies. Even though usability is an important aspect of these projects, the conflicts we address in this paper are not explicitly considered.

Furthermore, usable privacy cannot come without usable security, as security measures are used to implement privacy. Existing literature on usable security shows that the user is an important part of modern security chains. The strongest technical security measure is not effective, if attackers can circumvent them by means of social engineering. Well-known case studies analyze the usability of email encryption with PGP [27], of file sharing with Kazaa [9], and of authentication mechanisms and password policies [4, 12]. However, such case studies are specific to one PET or application and do not consider privacy conflicts arising from the PETs. Design principles for usable, yet secure systems [8, 11] focus on the development of usable security systems by supporting developers and emphasizing the importance of considering the user. Those principles could be extended or adapted based on our discussion.

2.2 Quality Models & Quality Conflicts

Technical and organizational security and privacy measures always have an influence on different quality aspects of tools and processes. A typical example is that cryptographic measures oftentimes have a negative impact on performance. However, there is a large variety of characteristics (e.g., from ISO 25010:2011, ISO 9001:2015, Gokyo Ri [15] and the Standard Data Protection Model [26]) that security measures can effect positively and/or negatively. To this respect, the conflicts discussed in this paper particularly focus on negative effects of the transparency and privacy measure "Privacy Dashboard" on security and data protection qualities.

A related, but more general and human-centered problem is the so-called privacy paradox. The privacy paradox describes the conflict between the need for privacy and the actual behavior of users with respect to taking privacy-related actions and technologies. Since this conflict is already widely considered in literature, we will exclude it from our work. Kokolakis et al. [16] surveyed the state of the art regarding the privacy paradox.

3 PRIVACY DASHBOARDS FOR TRANSPARENCY AND SELF-DETERMINATION

In this section, we take a look at the legal situation, especially the General Data Protection Regulation (GDPR), and the state of the art and practice. We then derive the most important use cases for privacy dashboards from it. In addition, we discuss stakeholders, requirements and special characteristics of privacy dashboards that are used in the working context.

3.1 Requirements and Legal Background

The GDPR strengthens the rights of European citizens regarding their privacy and protection of their data. GDPR requires companies to process personal data carefully and to obey data owners the rights for transparency, to access their data, to correct their data, to be forgotten, to be informed about data processing, to restrict data processing, to object data processing, not to be subject to automated individual decision-making and for data portability.

3.2 State of the Art and Practice

The GDPR provides general guidelines and does not deal with the concrete implementation. Tools to protect privacy or to enforce privacy settings are generally referred to as Privacy Enhancing Technologies (PETs). There are many tools, for example anonymization networks (e.g. TOR) or anonymization procedures in databases, for example based on differential privacy [6] and k-anonymity [24].

As a sub-category of PETs, there is a variety of tools tackling transparency issues, so called Transparency Enhancing Technologies (TETs). Hedbom [10] and Janic et al. [13] provide overviews and a classification of different (generic) TETs. Privacy Insight [2] is a transparency dashboard that displays data collection, usage and storage in graphs. However, it has not yet been evaluated in an industrial context or optimized for employees as users. Furthermore, it does not offer any possibilities for self-determination or enforcement of users' privacy needs. The Karlstad University presented the tool "Data Track", an approach to visualize the transfer of data [1], and researched the special requirements for privacy dashboards in cloud environments [7]. General requirements and a prototype implementation were researched by the Telekom Innovation Laboratories in Berlin [21]. Together with the Mozilla Corporation, the Technical University of Berlin conducted research on a user-friendly privacy dashboard for Firefox OS [18], which explains to users various functions of mobile devices that disclose personal data and which can be used to restrict data usage. The University of Oslo has presented an identity dashboard [23] that gives users an overview of the use of different digital identities and the data associated with them. The University of Freiburg published work on the classification of privacy dashboards [28] and an empirical analysis of their acceptance [3].

3.3 Privacy Dashboard Use Cases

Privacy dashboards ease the compliance to the GDPR by implementing the following rights that enable users to centrally

(1) inform about the processing of the user's personal data in general,
(2) inform about the processing of the user's personal data,
(3) view the user's personal data,
(4) request the erasure of the user's personal data,
(5) request the correction of the user's personal data,
(6) export the user's personal data (data portability and backup),
(7) configure privacy settings,
(8) give or refuse consent to data processing,
(9) getting notified about personal data breaches.

Thus, we consider these as our main use cases. From our discussions with different stakeholders, especially the data subjects, it became obvious that they want to exercise these use cases centrally and uniformly. Privacy dashboards follow exactly this approach. The scope of a privacy dashboard is always limited to, for example, a specific service (e.g., Twitter), a number of services (e.g., the Google privacy dashboard that covers all Google products), a company (e.g., the workplace privacy dashboard we have in focus), or a specific domain (e.g., personalized advertisements).

Privacy dashboards are primarily supposed to keep users up-to-date (transparency) and give them easy access to the privacy functions the user needs (self-determination). Based on these main use cases, the components of such a privacy dashboard are a knowledge base, data management, consent management, and communication. The knowledge base stores information about regulations regarding data processing (cf. use cases 1 and 2 and Figure 1).

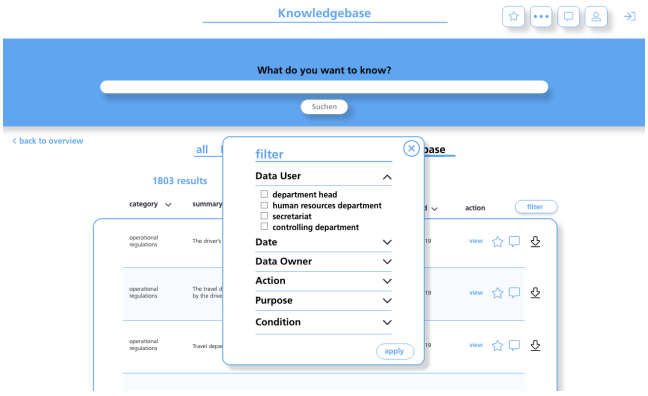

Figure 1: Dashboard Mockup: Knowledge Base

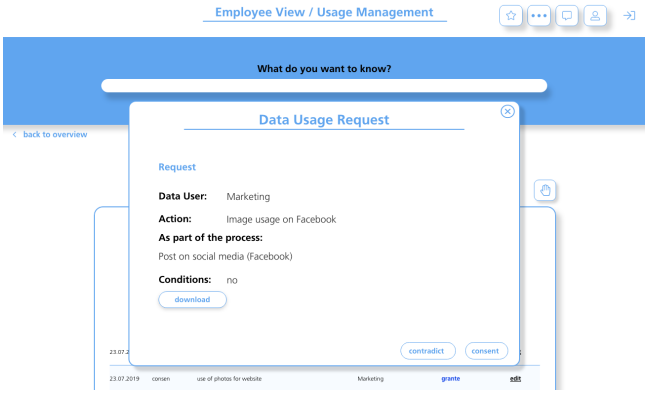

Figure 2: Dashboard Mockup: Data Usage Request (Consent)

The data management system provides an overview of the own data stored and processed in the organization and provides features for requesting the export, erasure and correction of data (cf. use cases 3, 4, 5, and 6).

The consent management system offers users privacy settings for general privacy rules (cf. use case 7) and allows them to request or give consent (cf. use case 8 and Figure 2) for more specific situations.

Finally, the company (e.g., the companies data protection officer) can inform users about personal data breaches via the dashboard (cf. use case 9 and Art. 34 GDPR), in addition to information via direct channels, such as e-mail.

3.4 Application Scenario: Workplace Privacy Dashboards

In a business context, privacy dashboards can be offered to customers (B2C), but also to a company's employees. In the project "TrUSD" [25], we focus on the latter case and develop a concept for workplace privacy dashboards. Like a B2C privacy dashboard, this worpkplace privacy dashboard is supposed to implement the users' right of transparency and self-determination and to enable the company to comply to legal regulations. We particularly focus on German small and medium-sized companies and the situation in Germany in general.

Major specialities of workplace privacy dashboards stem from regulations and the relationship between dashboard users and the company. Legal regulations, such as the GDPR, generally also apply to employees. However, article 88 allows member states to provide more specific rules for the context of employment. In a workplace environment, many personal data of employees simply have to be processed to administer a company. Some of these processes are even required by laws that overrule the data protection laws. This situation aggravates the understanding whether one's own personal data are processed legally compliant. Moreover, in comparison to B2C dashboards, the data users and data subjects often know each other and are in complex relationships and interdependencies.

3.4.1 Requirement Elicitation. In order to elicit requirements for workplace privacy dashboards, we conducted twelve workshops with members of different German companies and research institutes, an interview session, and a comprehensive literature research. More details about our requirements model and elicitation formats can be found in [20]. In total, we identified 49 stakeholders and collected 35 transparency needs, 7 self-determination needs, 39 data usage needs, 81 user requirements, 30 success criteria, 45 introductory requirements, 19 support requirements, and 71 categories of personal data involved.

3.4.2 Stakeholders. There are a lot of parties that have a stake in workplace privacy dashboards. The primary stakeholder group are *employees* who are data subjects. In addition to the employee himself, various other stakeholders are interested in ensuring that processing takes place in compliance with the law - including bodies such as a *supervisory board*, the *management* or the *workers' council*.

On an abstract level, data is processed by "the *employer*". On a closer look, however, a distinction must be made between automatic processing, processing by (other) employees, and external commissioned data processing. The middle case is particularly interesting for us, because the employee is a double role—being both data user and data subject.

Besides our primary stakeholders, there are a lot of secondary stakeholders involved. These do not use the dashboard themselves, but still have interest or influence on it. These include *legislation*, *B2B service providers* (e.g., auditors, processors, suppliers), *authorities* (e.g, safety authorities, supervisory authorities, chamber of industry and commerce), but also *external persons* (e.g., customer, press).

3.4.3 Demands & Requirements. Data subjects (employees) want to have an overview of all their personal data existing within the company. They would like to see which person in their company has

which usage permission for which of their data and for which purpose. In addition, they want to be actively informed when certain data are actually used (e.g., accessed, forwarded, deleted). Furthermore, employees request an overview and management capabilities for all privacy-relevant information, including permissions, usages, (missing) consents and data retention times.

In general, employees expect their employers to handle their data in a legally compliant and trustworthy manner. This includes secure and privacy-friendly defaults. Besides, the most frequently demanded requirement was the possibility to give explicit consent for certain usages. Furthermore, employees want the option to delete or correct their data.

Employees want to have a centralized tool with a GUI to manage all of their privacy settings and information and to directly access their personal data. However, some of them also want privacy-relevant information to be shown outside the dashboard, directly integrated into their work processes. Critical information should always be explicitly highlighted in the dashboard. Data export functionality and barrier-free accessibility to the dashboard was also demanded.

Employees want their data to be protected. However, they themselves do not want to spend much time and effort on protecting their data. Thus, they want to be informed actively by configurable notifications.

3.5 Derivation of conflicts and solution strategies

All our requirements were reviewed and consolidated within the project consortium. The consolidated requirements revealed conflicts between stakeholders, which made us aware that privacy dashboards could lead privacy ad absurdum. This was the starting point for us to considered other aspects of the dashboard critically, too.

A further strand, which we followed to identify conflicts, deals with the influence of concrete security and data protection measures on different quality characteristics. A measure can potentially improve a quality, worsen it, or both. For example, measures promoting transparency can improve confidence, but also worsen it when dubious practices are unveiled.

For this publication we have selected examples of conflicts and solutions that we felt were particularly worthy of discussion. We are interested in the opinion of practitioners and other researchers regarding the relevance and severity these conflicts and the applicability of the suggested solutions.

4 INHERENT CONFLICTS

In this section, we present five conflicts that may arise when using or introducing workplace privacy dashboards. For each conflict, we first describe what an "ideal" dashboard would look like from an employee's perspective (e.g., comprehensive transparency). "Ideal" here refers to the complete and comprehensive implementation with regard to one of the user's main requirements. We then discuss which privacy problems this "ideal" dashboard could cause, and present strategies how to resolve or mitigate these problems. For our discussion, we take the perspective of Alice, who is an employee at AnyCorp Inc. and data subject. Her colleague Bob takes the role of the data user, i.e., he processes Alice's personal data. We further assume that Bob processes the data within the scope of his duties (e.g. as an administrative employee who prepares Alice's pay slip) and not for illegitimate purposes (e.g. stalking or performance monitoring beyond the applicable regulations). However, it is important to mention, that Bob is also data subject with respect to his own data, and depending on Alice's role in the company, she can be data user as well.

4.1 Transparency vs. Data Minimization

4.1.1 Ideal Dashboard. An ideal privacy dashboard increases transparency by informing Alice about which of her personal data AnyCorp has access to and how her data is processed by the organization (cf. use cases 1 and 2). In particular, transparency requires "measures that—depending on the type of data to be protected—ensure that the processes of elicitation, processing and usage are comprehensible, verifiable and assessable with reasonable effort." [22]. For instance, the privacy dashboard provides information about which of Alice's personal data was updated by Bob (in fulfilling his role at AnyCorp). Thus, the dashboard also encourages digitization.

4.1.2 Problem. In order to provide comprehensive transparency, many actions that Bob performs (e.g., data access, data processing, data deletion) have to be automatically monitored and logged by AnyCorp. For example, if Bob updates Alice's personal data, this event—including Alice's ID and Bob's ID and action—has to be logged. Thus, the event itself is person-related with respect to both employees. The greater or more precise the transparency is, the more person-related data needs to be collected. This collection, however, conflicts with the principle of data minimization. Moreover, a dashboard itself counteracts data minimization; the privacy dashboard is yet another system storing data, which are partly already available in other systems. The challenge is, to balance the principles of transparency and data minimization, which are both central aspects of the EU-GDPR.

4.1.3 Solution Strategies. First, the dashboard itself should store as few data as possible. Instead, it should be integrated with other (legacy) systems that need to store the personal data anyway and serve as some kind of proxy. Second, Alice should be provided with exactly the data she actually needs—no less, but also no more. Of course, users require different levels of detail to experience transparency. In a survey, which we conducted, some employees indicated that they only like to have abstract information about the processing of their data, e.g. which department processes it [20]. Others would like to know the exact person which is processing their personal data since they do not trust all colleagues alike. Thus, the privacy dashboard should be tailored to the user's concrete needs. To determine this level (which might differ for different user groups), precise studies are necessary. In addition, as with other data, specific and appropriate deletion periods must be established, and anonymization might be a possible strategy as well for some use cases.

4.2 Transparency vs. Surveillance

4.2.1 Ideal Dashboard. An ideal privacy dashboard offers Alice comprehensive transparency by informing her directly when her

personal data was used (cf. use case 2). The dashboard informs her at which time personal data (e.g., a picture) was used for a certain purpose by which of AnyCorp's employees, e.g., by Bob. In this way, Alice can check whether personal data has been used lawfully (e.g., Bob uploaded the picture to social media) and in case of a violation, she can initiate countermeasures directly.

4.2.2 Problem. The problem is that the combination of time (when) and user (who) can also be used to monitor work and work performance. From the data, one could see when or how often Bob accessed or processed a data item and make conclusions about his work. For example, the access date clearly indicates when Bob was working. If the gathered information can indeed be used against Bob, he will most likely not accept the dashboard anymore. Bob could then be trying to evade surveillance, e.g., by using local copies which the dashboard does not observe. This poses a threat to data security counteracting the goals of the dashboard.

4.2.3 Solution Strategies. This problem can partly be solved with anonymization procedures. As soon as no personal reference can be established, there is no longer any danger of surveillance. If personal reference is mandatory for a particular use case, a trade-off must be made between the transparency requirements of Alice and the anonymity of Bob, especially if Alice has a superior role. One solution strategy is the aggregation of data. For instance, Alice could get a summary at the end of the day telling "your ID was processed by Bob today" instead of "Bob processed your ID at 1:54am and at 3:32pm". The problem, however, is that some use cases only make sense with personal and concrete data. In this case, it is perfectly feasible to deactivate the entire transparency function for Alice. Incidentally, even consent is of limited help at this point, as it can lead to social pressure. We will discuss this later in the section "Self-Determination & Social Pressure".

4.3 Central Entry Point vs. Central Attack Point

4.3.1 Ideal Dashboard. Dashboards are—by definition—central tools. From a usability point of view, this centrality brings immense advantages and was demanded by most employees and also the employer during our requirements workshops. Alice knows, where to find all information from internal regulations to their personal data. Moreover, Alice only needs to sign up a single time, the structure of the presented information is consistent and therefore easy to grasp. According to the requirements we elicited in our project, the ideal dashboard is available anytime, anywhere and allows users to inform themselves or act quickly and easily. This includes access via mobile devices and apps, including—at least partial—offline capability.

4.3.2 Problem. However, such a centrality is also a security risk, as it provides a single point entry point for attackers. This is especially critical and tempting, as the dashboard provides interfaces for data deletion, correction and export (cf. use cases 4, 5, and 6). Small vulnerabilities or flaws can have drastic effects and endanger not only Alice's, but everyone's privacy if an attacker gains access to personal data from or via the dashboard. Central systems are attractive targets, since intrusion can give access to a large amount of data. The attacker only has to focus on one point of attack, which makes attacks a lot easier for them.

4.3.3 Solution Strategies. First, central services should not be designed in a monolithic way, even if this sounds particularly tempting for dashboards. Layered architectures, micro-services and similar concepts allow appropriate scalability and reliability. This also has advantages for data confidentiality. If an attacker gets access to the database of a micro-service, the data of the other services remain protected—provided that the services are appropriately protected and separated from each other. Second, it can also make sense to cut back on offline capability. Finally, it is rarely necessary or useful to grant remote access to privacy dashboards in the work context. In particular, access via private hardware is mostly not allowed anyway. Thus, a VPN connection to a secure company network may be assumed here, as it significantly reduces the probability of a successful attack and the resulting disadvantages (e.g. in terms of usability) are tolerable. Time-critical notifications can still be delivered without VPN via other channels (e.g. via SMS).

4.4 Self-Determination vs. Social Pressure

4.4.1 Ideal Dashboard. One main goal of the dashboard is to empower employees to determine the information who is allowed to use which data for which purpose. Self-determination is of course generally desirable and should be implemented whenever possible.

4.4.2 Problem. There are cases in which social pressure can arise from these freedoms. If Alice is always the only person in a web-meeting who objects to the recording of the meeting, she could be quickly stamped or ridiculed. This problem occurs mainly when Alice's privacy settings (including consents) are obvious to others. This can happen explicitly, but also implicitly. If the video recording of a meeting is not possible whenever Alice is present, the conclusion that Alice has not given her consent is trivial. Furthermore, if Alice does not consent to data processing, her colleague Bob might not be able to complete his tasks as mandatory information is not available. This can additionally increase the social pressure on Alice.

4.4.3 Solution Strategies. Explicit disclosure of privacy information can of course be excluded by visibility regulations or anonymization procedures. In the case outlined, however, this would not help, as the data disclosure is rather implicit. These implicit information flows can hardly be solved technically. Especially in the area of employee data protection, however, company agreements can be made which make individual decisions superfluous—at the expense of Alice's self-determination, of course. At this point, the workers' council has an important task (if there is one in the company). It is its task to represent the interests of all employees and to work out suitable regulations and compromises. This also corresponds to the common view that individual consent in the working environment should be avoided if possible.

4.5 Trust vs. Mistrust

4.5.1 Ideal Dashboard. An ideal dashboard should strengthen the trust relationship between Alice and AnyCorp. Alice experiences that AnyCorp cares about her and empowers her by providing high

transparency and data sovereignty. This might even attract job candidates.

4.5.2 Problem. Extremely comprehensive transparency naturally entails the risk of uncovering things that lead to mistrust. Even though all parties may take the greatest care in handling personal data, reasons for the data processing may sometimes not be directly apparent and lead to mistrust. This is one reason why companies sometimes hesitate to offer this level of transparency—at least to the outside world. They do not want to be pilloried, although they actually take data protection very seriously. Paradoxically, however, data subjects (e.g., Alice) then wonder whether the company has something to hide. Feelings of mistrust could also emerge, if Alice or her representatives (e.g., workers council) are not involved in the process of introducing the dashboard to an organization. If Alice is suddenly confronted with the dashboard without being familiar with its purpose and how to use it, she might be skeptical about it and smell an ambush.

4.5.3 Solution Strategies. Independent of the dashboard, to improve the relationship between employees and employer, the employer must primarily do its best to secure the employees' data, comply with the earmarking, and do not hide any information about data processing. A good corporate culture, legally compliant processing of employee data and tact when introducing new technologies solve most problems here. Nevertheless, critical questions will always arise, also (but not exclusively) because privacy dashboards can never be perfect. Despite the best efforts of all sides, data can be incomplete or outdated. Also at this point, it is important to deal with this problem openly and constructively. After all, trust should be the basis of every employment relationship and technical tools should not replace personal contact.

4.6 Summary

Figure 3 gives on overview on the conflict we described before. Maximizing transparency, self-determination, and availability for Alice is at first desirable and has several positive effects. On a closer look, however, the maximization of each aspect can have several side-effects—for Alice, for her colleagues and for the employer. Of course, not all effects are observable at the same time in practice and many effects are use-case-specific. In some cases, the effect can even be positive and negative at the same time.

Figure 3: Overview on Conflicts

5 CONCLUSION

The focus of this paper was to draw attention to an area of conflict that is often neglected. It is often discussed that security and privacy measures (such as PETs and TETs) can have negative effects on aspects such as usability or performance. However, the fact that they paradoxically can have negative effects on security or privacy is not discussed much in the literature. However, the conflicts discussed in this paper clearly show that this is indeed a realistic scenario.

Unfortunately, this also means that the "ideal" privacy dashboard does not, respectively cannot, exist. Even if the privacy dashboard initially appears ideal from the user's point of view and the user also uses it to implement his or her data protection, the introduction of such a tool alone leads to a large number of new problems. With reference to the privacy paradox, the question arises whether it is at all possible to resolve the issue in a meaningful way. Because regardless of whether a user exercises his data protection rights or not, someone's privacy is endangered in one way or another. The maxim that users should be given as much transparency and participation as possible is therefore not tenable. Instead, individual case considerations are indispensable.

We presented conflicts in the workplace environment. As mentioned in section 3.5, B2C and corporate privacy dashboards differ regarding certain aspects. Nevertheless, the conflicts "'Transparency vs. Data Minimization"', "'Central Entry Point vs. Central Attack Point"' and "'Trust vs. Mistrust"' are also applicable in the B2C context.

The example conflicts presented in this paper are neither complete, nor are the solution strategies universal. We currently identify similar relationships and conflicts in the context of creating a joint quality model for usable security. Based on this model, and further case studies, we are going to refine also the solution strategies. This will make it possible in the future to be aware of potential conflicts, to reduce them or at least mitigate them.

ACKNOWLEDGMENTS

The research presented in this paper has been supported by the German Ministry of Education and Research project "Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen (TrUSD)" (grant no. 16KIS0898). The sole responsibility for the content of this paper lies with the authors.

REFERENCES

[1] Julio Angulo, Simone Fischer-Hübner, Tobias Pulls, and Erik Wästlund. 2015. Usable Transparency with the Data Track: A Tool for Visualizing Data Disclosures. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI EA '15)*. Association

for Computing Machinery, New York, NY, USA, 1803–1808. https://doi.org/10.1145/2702613.2732701

[2] Christoph Bier, Jürgen Beyerer, and Kay Kühne. 2016. PrivacyInsight: The Next Generation Privacy Dashboard. In *Privacy Technologies and Policy : 4th Annual Privacy Forum, APF 2016, Frankfurt/Main, Germany, September 7-8, 2016 ; Proceedings. Ed.: Stefan, Schiffner (Lecture Notes in Computer Science)*, Vol. 9857. Springer, Cham, 135–152. https://doi.org/10.1007/978-3-319-44760-5_9 46.12.03; LK 01.

[3] Johana Cabinakova, Christian Zimmermann, and Günter Müller. 2016. An Empirical Analysis of Privacy Dashboard Acceptance: the Google Case. In *24th European Conference on Information Systems, ECIS 2016, Istanbul, Turkey, June 12-15, 2016*. Research Paper 114. http://aisel.aisnet.org/ecis2016_rp/114

[4] Yee-Yin Choong and Mary Theofanos. 2015. What 4,500+ People Can Tell You – Employees' Attitudes Toward Organizational Password Policy Do Matter. In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (Eds.). Springer International Publishing, Cham, 299–310.

[5] Council of European Union. 2014. Council regulation (EU) no 269/2014. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1416170084502&uri=CELEX:32014R0269.

[6] Cynthia Dwork. 2006. Differential Privacy. In *Automata, Languages and Programming*, Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 1–12.

[7] Simone Fischer-Hübner, Julio Angulo, and Tobias Pulls. 2014. How can Cloud Users be Supported in Deciding on, Tracking and Controlling How their Data are Used?. In *Privacy and Identity Management for Emerging Services and Technologies*, Marit Hansen, Jaap-Henk Hoepman, Ronald Leenes, and Diane Whitehouse (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 77–92.

[8] Simson Garfinkel. 2005. *Design principles and patterns for computer systems that are simultaneously secure and usable.* Ph.D. Dissertation. Massachusetts Institute of Technology.

[9] Nathaniel S. Good and Aaron Krekelberg. 2003. Usability and Privacy: A Study of Kazaa P2P File-Sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, Florida, USA) *(CHI '03)*. Association for Computing Machinery, New York, NY, USA, 137–144. https://doi.org/10.1145/642611.642636

[10] Hans Hedbom. 2009. A Survey on Transparency Tools for Enhancing Privacy. In *The Future of Identity in the Information Society*, Vashek Matyáš, Simone Fischer-Hübner, Daniel Cvrček, and Petr Švenda (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 67–82.

[11] Luigi Lo Iacono, Matthew Smith, Emanuel von Zezschwitz, Peter Leo Gorski, and Peter Nehren. 2018. Consolidating Principles and Patterns for Human-centred Usable Security Research and Development. In *European Workshop on Usable Security, London*.

[12] Philip G. Inglesant and M. Angela Sasse. 2010. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 383–392. https://doi.org/10.1145/1753326.1753384

[13] Milena Janic, Thijs Veugen, and Jan Pieter Wijbenga. 2013. Transparency Enhancing Tools (TETs): An Overview. *Workshop on Socio-Technical Aspects in Security and Trust, STAST*. https://doi.org/10.1109/STAST.2013.11

[14] Sabrina Kirrane, Javier D Fernández, Wouter Dullaert, Uros Milosevic, Axel Polleres, Piero A Bonatti, Rigo Wenning, Olha Drozd, and Philip Raschke. 2018. A scalable consent, transparency and compliance architecture. In *European Semantic Web Conference*. Springer, 131–136.

[15] Ralf Kneuper. 2015. Messung und Bewertung von Prozessqualität – Ein Baustein der Governance. *HMD Praxis der Wirtschaftsinformatik* 52, 2 (2015), 301–311. https://doi.org/10.1365/s40702-014-0079-z

[16] Spyros Kokolakis. 2017. Privacy Attitudes and Privacy Behaviour. *Comput. Secur.* 64, C (Jan. 2017), 122–134. https://doi.org/10.1016/j.cose.2015.07.002

[17] Roman Matzutt, Dirk Müllmann, Eva-Maria Zeissig, Christiane Horst, Kai Kasugai, Sean Lidynia, Simon Wieninger, Jan Henrik Ziegeldorf, Gerhard Gudergan, Indra Spiecker gen. Döhmann, Klaus Wehrle, and Martina Ziefle. 2017. myneData: Towards a Trusted and User-controlled Ecosystem for Sharing Personal Data. In *INFORMATIK 2017*, Maximilian Eibl and Martin Gaedke (Eds.). Gesellschaft für Informatik, Bonn, 1073–1084. https://doi.org/10.18420/in2017_109AddtoCitaviprojectbyDOI

[18] Marta Piekarska, Yun Zhou, Dominik Strohmeier, and Alexander Raake. 2015. Because we care: Privacy Dashboard on Firefox OS. arXiv:cs.CR/1506.04105

[19] Antti Poikola, Kai Kuikkaniemi, and Harri Honko. 2015. Mydata a nordic model for human-centered personal data management and processing. *Finnish Ministry of Transport and Communications* (2015).

[20] Svenja Polst, Patricia Kelbert, and Denis Feth. 2019. Company Privacy Dashboards: Employee Needs and Requirements. In *International Conference on Human-Computer Interaction*. Springer, 429–440.

[21] Philip Raschke, Axel Küpper, Olha Drozd, and Sabrina Kirrane. 2018. *Designing a GDPR-Compliant and Usable Privacy Dashboard.* Springer International Publishing, Cham, 221–236. https://doi.org/10.1007/978-3-319-92925-5_14

[22] Martin Rost and Kirsten Bock. 2011. Privacy By Design und die Neuen Schutzziele. *Datenschutz und Datensicherheit - DuD* 35, 1 (01 Jan 2011), 30–35. https://doi.org/10.1007/s11623-011-0009-y

[23] Jonathan Scudder and Audun Jøsang. 2010. Personal Federation Control with the Identity Dashboard. In *Policies and Research in Identity Management*, Elisabeth de Leeuw, Simone Fischer-Hübner, and Lothar Fritsch (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 85–99.

[24] Latanya Sweeney. 2002. K-Anonymity: A Model for Protecting Privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.* 10, 5 (Oct. 2002), 557–570. https://doi.org/10.1142/S0218488502001648

[25] Jan Tolsdorf, Christian K Bosse, Aljoscha Dietrich, Denis Feth, and Hartmut Schmitt. 2020. Privatheit am Arbeitsplatz. *Datenschutz und Datensicherheit-DuD* 44, 3 (2020), 176–181.

[26] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. 2020. Das Standard-Datenschutzmodell (SDM). https://www.datenschutzzentrum.de/sdm/

[27] Alma Whitten and J. D. Tygar. 1999. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8* (Washington, D.C.) *(SSYM'99)*. USENIX Association, USA, 14.

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