An overview over Inverse Transparency

Mahaut Gérard (mahaut.gerard@tum.de)
Seminar Inverse Transparency (WS 21/22)
Advisor: Valentin Zieglmeier

Abstract

Digital interfaces are everywhere. They tend to give us comfort, communication, or help us to achieve tasks. There are undeniable parts of everyone's life both in the private life and in the workplace. This goes with an always increasing amount of data. This increasing number of data can enhance (online) experience. However, this can also be a severe threat to our privacy as well as data misuse. To tackle this issue, several solutions appear from absolute data minimization to transparency. One of these solutions is the concept of Inverse Transparency, which aims at being a compromise to answer all issues.

Preserving data relevant usage and addressing data misuse is inherent to the concept of data transparency. The question of privacy along with transparency is addressed here.

We also explore, with a survey, the relations and differences of the concept of Inverse Transparency in the workplace and private life. Data have their use in both, however, related goals, consequences, and power balance may appear to vary. We find that the scalability of the concept, initially thought for the workplace, is not straightforward for private life.

1 Introduction

Today, there are a lot of data created and processed which have a large number of advantageous applications. This large amount of data collected is enabled by the widespread use of the internet (almost everybody uses internet and then creates data), the decreasing cost of data based technologies, and the multiplication of them. However, this comes with a threat to our privacy and (a risk of) data misuse. Because of these potential harmful issues, the digital environment may appear to be untrustworthy. Several institutions built regulations addressing this point. For example, EU has created the General Data Protection Regulation [1] (GDPR) and California have the California Consumer Privacy Act [2] (CCPA). These are instances of laws that can lead towards data minimization. Data minimization states that only necessary data should be processed and collected. It addresses previous concerns by preventing them from possibly happening. Therefore, data minimization appears to be a solution to today's data usage. And maybe this is the only acceptable solution for sensitive data, like personal health data [1].

For non-sensitive data, other solutions may arise. Another (easy) solution may be to continue as of today. The advantage is that all relevant data processing and data-based innovations can continue without any change. However, in that case, data misuse is also facilitated, privacy stays vulnerable and the environment stays untrustworthy.

This is in this context that the Inverse Transparency [2] concept is born, designed for the workplace. This concept may be another solution (in the workplace), at the overlapping zone of privacy, data usage, and transparent data usages. In a way, it claims to take all the advantages and no disadvantages outlined before. We will do an overview of this third solution in the rest of the paper.

Figure 1 summarizes this present situation of data usages and these perspectives for the future.

After explaining the concept of Inverse Transparency, we detail the technical components on which Inverse Transparency is based. We see that it can, to some extends, question privacy. Finally, we explore the implication of the Inverse Transparency concept in two different areas, namely workplace and private life. Our work tries to address the following motivation questions:

Q1: What is Inverse Transparency?
Q2: What related research exists?
Q3: What are the related tools?
Q4: Does it participate in more data privacy?
Q5: Does this concept also make sense in private life?

In this paper, we consider the workplace and private life environments separate, as shown on Figure 1. For *Q5*, we want to address the differences that arise when talking about Inverse Transparency in the private life and in the workplace. We operate a dichotomy between these environments. How-

[1] https://gdpr-info.eu/
[2] https://oag.ca.gov/privacy/ccpa

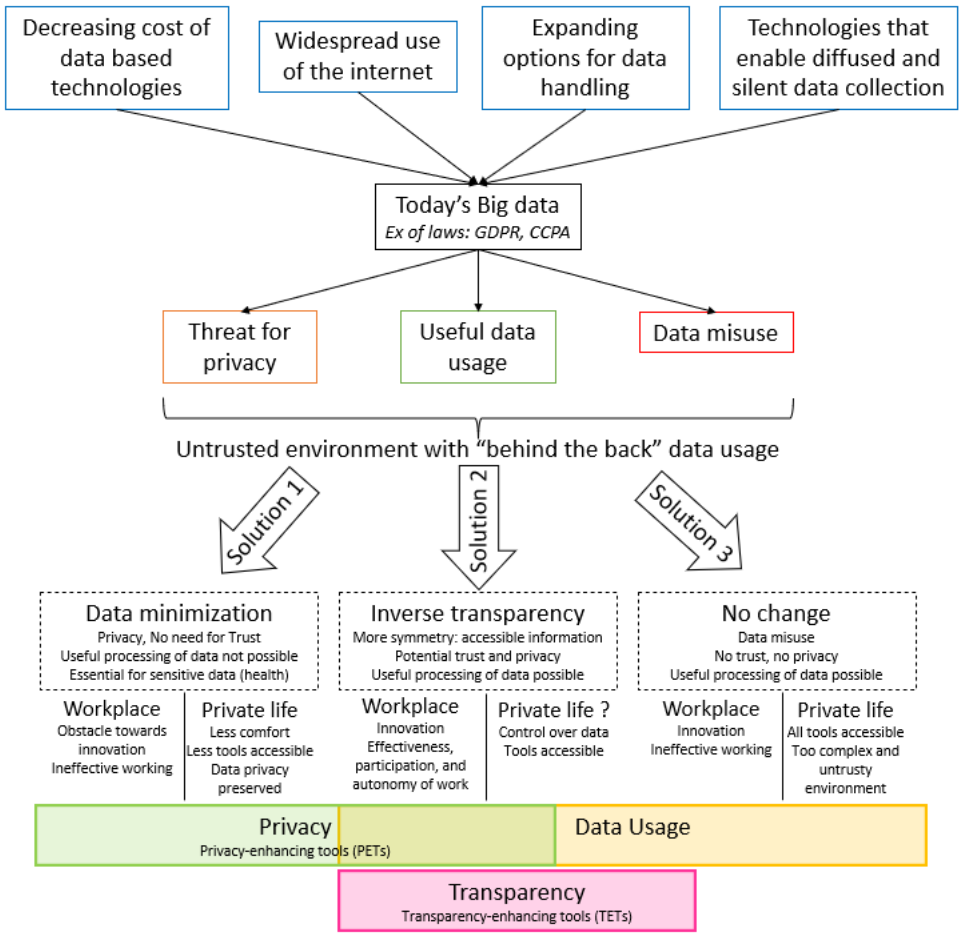

Figure 1: This graph puts into perspective issues related to today's data usage (up layer), three possible solutions to tackle these issues (intermediate layer), and their link to privacy, data usage, and transparency (bottom layer).

ever, for other discussions, these two environments should be considered together.

2 Related works

The concept of transparency is now explored by more and more research and required by public opinion in some fields. After political scandals, for instance, public opinion often asks for more openness and transparency. They see it as a path through authentic information; in fact, as a path combining information availability and information quality [3]. Introna opposes transparency to privacy as in the workplace employers' general interest is to maximize transparency while employees' interest is to maximize privacy. Transparency claims of employers are based on collective thinking, productivity, resources allocation or ensuring that the employer's money is well used. Whereas privacy claims of employees are based on data misuse, trust or personal data control. While claims for privacy and claims for transparency are equally reasonable, employee position is of severe power asymmetry and therefore fairness should be addressed in the first place [4]. Mayer stresses that employers should consider these issues as transparency contains risks for them too. The risks are loss of trust, growing pressure, and oversight of the complexity of data evaluation. Pulls proposes two privacy-preserving transparency enhancing tools to make transparency compatible with privacy. Transparency then seems not to be de facto opposed to privacy. However, for Janssen and van den Hoven realization of both transparency and privacy is the challenging part.

Other research takes transparency to address the privacy vs. performance trade-off. Trask et al. propose *Structured Transparency* to benefit both from data analysis and data privacy. They present five main components to enforce desired information flows with a clearly-defined data desiderata. Gierlich-Joas et al. present *Inverse Transparency* as tackling these trade-offs. In fact, the conflict between data privacy and data-based use cases is the starting point of many researches [1, 2, 7, 8]. Zieglmeier and Pretschner add the users' trust consideration. They argue that the trust parameter is important as it influences how a tool is utilized. Transparency appears to be a key element to increase trust. In addition, Flavian and Guinalíu emphasize that the *perceived* security and privacy influence the final user trust. The concepts of transparency, privacy and trust are interrelated in many research. They should be addressed keeping in mind the final user's perception. The term *data sovereignty* developed by [11] is another way to approach the problem of data privacy concerns versus highly personalized interaction for which data is essential. Data sovereignty corresponds to the right to dispose of its own personal data. Dabrock presents two components to effectively implement data sovereignty: a data agent to automatically implement user's preferences and a data trustee to compare the preferences with the actual processing of data.

3 The concept of Inverse Transparency

The first time Inverse Transparency is mentioned is in the 1998 novel of Brin [9]. However, the concept of Inverse Transparency we talk about here was introduced by the project "Inverse Transparenz" [2]. This inter-disciplinary project was thought for the workplace. It combines sociology, leadership, and IT research as well as practical tests and executions. Figure 2 summarizes the main parts of this project. We will discuss in the seventh section the difference that may arise when considering this concept for private life. However, we discuss in this section the concept from a workplace point of view. The two core ideas are:

1. Make data transparent
2. Consequently, inform each person on which personal data is generated and how it is processed

Inverse Transparency addresses the conflict between data protection and data-based use cases. It enables data-based use cases as all data stay accessible. It appears to enable data protection as all data access is transparent and therefore makes data misuse unattractive. This represents the *Watch the Watcher* principle. Compared to transparency, Inverse Transparency implies higher employee participation. In fact, with Inverse Transparency, employees are able to control the accessibility, collection or enable further usage of their personal data [9]. In short, enable employees to participate in data protection and management. The concept tries to profit from transparency (facilitated by an increasing number of tools) in a positive way. That is to say, trying to avoid workplace surveillance, even though transparency tools make it easier, and in the same time building innovative work and leadership process. In fact, Inverse Transparency aims at employee autonomy by giving them the means to actively use data and improve their own work. This idea of autonomy tends to use data transparency not as a surveillance tool but as a work and organizational tool. [2]

The key point of Inverse Transparency towards limiting data misuse is the symmetrization of power. Of course in the workplace, the symmetrization of power can't be total and is in fact complex. It can't be total giving that an employer has always the power to discharge an employee, for example. It is complex as several levels of power appear and also depend on the job market. Employees also have some forms of power: structural (one can change job, or participate in strike), associational (work council), and institutional (laws that protect employees) [12]. The idea of Inverse Transparency is to diminish the asymmetry of power linked to information asymmetry. In the workplace, employers have almost always more power than their employees. In a lot of countries, the law restricts the right of employers to look at their employees' data. In Europe, this is for example the GDPR. However, in the current system employers can easily look at their employees' working data,

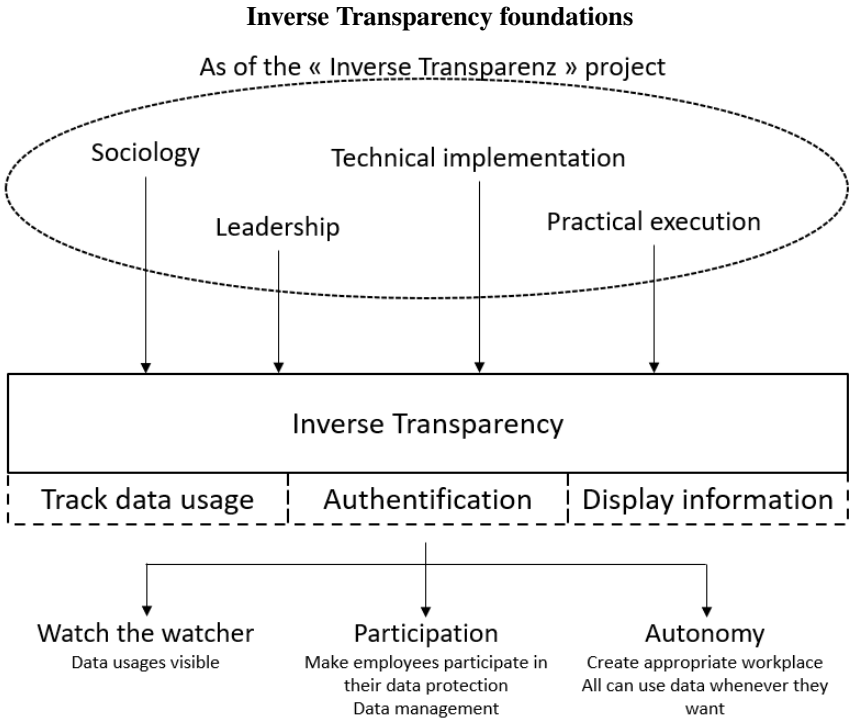

Figure 2: This graph presents the resource given to the "Inverse Transparenz" project (upper layer), the three mainstays of this concept which are data usage tracking, authentication, and information display (middle layer) as well as the expected outcome of the project in the workplace (bottom layer). [1, 2]

"behind their back" [13]. Consequently, it gives even more power to employers. Data strengthens power unbalance between employers and employees. It is here that comes Inverse Transparency: giving the possibility to employees to look at their data usages and to look at others' data. Employees have more information into their hand and *knowledge is power* [3].

4 Components of Inverse Transparency

Inverse Transparency is a concept that we have described previously. Concretely, this concept relies on a group of tools. This group is named transparency-enhancing tools or TETs. TETs are system-independent tools [14]. Their purpose is to inform data providers about how personal data is handled online. There are three mainstay components of transparency-enhancing tools needed in Inverse Transparency, for which Zieglmeier and Pretschner gives a possible implementation. To present to data providers their data usage, data usages have to be tracked (A), data usages have to be stored and data consumers have to be identified (B), an interface must display all the collected information (C). To this, we can add the management of data (D) by the data provider, who may want to delete some data or set his/her preferences for example. However, this last category may also belong to privacy-enhancing tools (PETs). Overall, the four categories of tools are interrelated and depend on each other. There is certainly an overlap between TETs and PETs, especially for the data control tools. However, here we consider PETs to be closed where TETs are open. In fact, PETs are preventive tools to reduce data processed before it is actually processed, there is no room for data usage. TETs are more open as their main purpose is to display information concerning data processed, thus after processing. We also note that TETs serve PETs as they help highlight data usage and make it possible for users to exercise their rights online. [6]

(A) *Data usage tracking*. This is the forefront component to guarantee transparency. It is named Monitor by [1] and aims to track every data usage. That is to say, what data each service provider processes and in the end what total information is processed [15] by all the service providers used. An implementation is also given by the TAMI project [16, p.9] in the field of data mining. This task can be compromised by screenshots or other, out of the Inverse Transparency system, data collection. For instance, if I screenshot a database containing personal data, I can create a separate copy that will consequently not be tracked. Therefore, this component on which rely (B) and (C) may be bypassed by malicious data users.

(B) *Authentication and data usage's storage*. This is the

[3] As this expression is often attributed to Francis Bacon, or lots of others https://www.brainyquote.com/topics/knowledge-is-power-quotes

component that refers to privacy and this is why cryptographic systems have been presented for this [6]. This is the Safekeeper presented by [1], which verifies authentication of the data user at each stage and stores monitored usages. The monitored usages come from the data tracking done by (A).

(C) *Display collected information*. This component may be an important part of users' trust feeling. The complexity of this component relies on the fact that there are a lot of data processed but that the interface displaying data must be easily understandable. As presented in [1], their *Display* component aims to make information transparent to data owners. The information displayed is based on the one stored by (B), therefore this component is dependent on the previous one. Plenty of other, often more general, tools exist [16, p.10-13], for example, Privacy Bird or Privacy Evidence. PrivOnto framework [17] is also to be cited as it makes website privacy policies approachable. This element enables data providers to control if (D) is well applied.

(D) *Data management*. Plenty of tools already exist in this category as the Google dashboard for Google services [6, p.11], or the Amazon book recommendation service [16, p.14] which enables users to define what should be taken into account for the future book recommendations. This tool enables users to set preferences and therefore set their own compromise between data privacy and data-driven use cases. This is the element related to the choice between data minimization and full data disclosure.

A lot of different TETs exist today, however, some limitations appear. First, there are not widely adopted by users, partly because there is a lack of instruments to inform people about them. Besides, users are not always aware of threats to their data privacy. Users simply do not know TETs existence and even if they knew wouldn't understand their utility. This is related to data and IT education. Second, they do not cover every aspects of data protection. For example, some articles of the GDPR are not covered by any TET. [14]

5 Where is the privacy?

In what we discuss above, they may be some points that question you about privacy [16]. Someone may ask: *If all data is transparent, then visible, there is no more privacy of data*. Another may wonder: *If I must log in to use data or provide data, then my identity is given and there is no privacy*. Some paper proposes TETs solution to answer both questions, [6] using cryptographic techniques and naming them Privacy-Preserving TETs. In detail, in this paper, Pulls proposes a cryptographic system for distributed privacy-preserving log trails and a system to destroy the chronological order of log entries. These address our second question of logging security. The paper also presents a system to disable the deduplication in order to avoid the linkability of files and users. Finally, a cryptographic system for privacy-friendly cloud storage is presented. However, few other works focus on these privacy questions.

6 Survey methodology

Data collection, usefulness and misuse of data are also part of private life. The concept of Inverse Transparency is originally developed for the workplace. However, since it appears that this concept is a compromise between the usefulness of data and the protection of individuals, we studied the scalability and usefulness of this concept in private life. We choose a qualitative research approach to access these questions. This approach enabled us to adjust the questions throughout the interviews were conducted. [13, 18]

6.1 Participants

We followed a purposive sampling approach, as in [13]. That is to say that we selected participants so that we have a heterogeneous sample in terms of age, gender and area of work. We also selected participants that are currently employed. So that we can ask questions both in the workplace and in the private life to each participant. Information on the participants' sampling is provided in Table 1. Our final sample includes 5 females and 5 males aged between 20 and 65 years. In order to have variations in perspectives and knowledge, we selected some employees with IT-related jobs (4 participants) and others without (6 participants). In the next sections, after each participant's quotation, we add the ID of the participant, from P1 to P10.

Table 1: Information on sample of participants

Parameter	Frequency
Age	
<30	4
30-50	3
>50	3
Gender	
F	5
M	5
IT related job	
yes	4
no	6
Total	10

6.2 Interviews

Interviews were held as one-to-one discussions via telephone calls or in-person meetings. We conducted 10 semi-structured interviews with open-ended questions. The interviews were conducted in France and done in French. All interviews were

recorded. There were two main parts in the interviews: first were the workplace-related questions and second were the private life related questions. The concept of Inverse Transparency was discussed in both parts. During the interviews and before mentioning Inverse transparency for the first time, the concept was introduced with a unique description. We guaranteed uniqueness by reading the description to each participant. This written description is equivalent to the way we presented the concept here. More general data privacy-related questions were also included in the interview. The main parts of the interviews are detailed in Table 2 as well as the specific questions we asked in every interview. Other questions asked to participants depend greatly on the participant, his data privacy concerns and awareness. In fact, the interviewer followed up on topics that arose naturally in interviews. Therefore, the content of the interviews vary. This was expected while choosing open-ended questions and one-to-one discussions interviews.

6.3 Analysis

We used a thematic analysis approach to analyze our interviews. First, we transcribed each audio recording on markdown files doing a French to English translation. All the rest of the process was then done in English. We then grouped answers by the same questions. For example, if one question was asked in several interviews, the different answers to this particular question were written under this question transcribed once. However, we kept the trace of the participant by mentioning the ID of each participant before each answer (Participant_ID: answer_question_A). Second, we generated codes for each answer. The codes aimed to describe, not interpret, the content of the answer. After this coding phase, we searched for themes in order to gather related codes. This was done in an iterative manner. Then, the themes were reviewed to address themes overlap and to verify that each answer corresponds well to its assigned theme. Finally, we named and defined themes. [19]

The findings of this analysis are taken into account in section 7, which addresses the scalability of the Inverse Transparency concept into private life.

6.4 Limitations

Our survey sample is heterogeneous in many different ways: age, gender and area of work. However, it could be interesting in future works to also have a heterogeneous sample in terms of the qualification of employees. In fact, our sample represents for the main part employees with high qualification and therefore managerial position. This is likely to have biased our sample answers. For example, one participant stressed that "I don't know how my work can be quantified simply as at my level I am paid to think not to implement" (P2). This assertion challenges the data one may have on hourly efficiency.

Table 2: Interview structure

Categories	*Always asked questions*
1. Workplace	
- Data Collection	*Do you know what kind of data is collected by your employer? Do you believe that he/she may collect more than that?*
- Trust	
- Power	
∼ Description of the Inverse Transparency concept ∼	
- Inverse Transparency	*What are your first thought concerning this concept?*
- Wishes	*Which data would you want to access?*
2. Private life	
- Inverse Transparency	*Would you like the same concept outside of the workplace, in your private life?*
- Data privacy concerns	*Are you concern by your data privacy?*
- Online practises: Cookies, Trade-offs, Browser, Google dashboard	
- Loyalty	
- GDPR	
- Wishes	*In a perfect world, what would you want for your data and its privacy?*

In fact, if your work consists of coding project features, one may check how many lines of code you implement in one hour. This is a quantifiable quantity. However, if your work consists of building the main architecture of a project after discussions with the client and redaction of a contract, such quantifiable quantities are more difficult to define. Another parameter to look at is the correlation between a person's knowledge of data collection and the person's way to manage data. In fact, in our survey, we focused on group of answers for each question but not on the homogeneity throughout each participant interview.

7 Workplace Inverse Transparency and private life Inverse Transparency

TETs and PETs are also available in our private sphere [16]. As described before, we conducted a survey on working people about their management and knowledge of data in their working space and their private space. For each theme, we present the answers for the workplace and private life, we then conduct a comparison between both. This gives some insight into the differences that arise when considering the concept in both environments. The main themes that arise from our survey analysis are the next subsections. The last subsection, taking technical consideration, is not based on our survey's findings. In the workplace, we take into account the employee-employer relationship. In private life, we focus on the data provider-data user relationship. That is to say a website and one of its users, an app and one of its users, a browser and one of its user or a device (for example, an Android smartphone) and one of its users.

7.1 Data types

Workplace Four main types of data were mentioned by the participants when asked about what data is collected in their company. We noted that the four categories were not equally cited by all participants. In fact, the two first categories were always specified by participants. Whereas the two last categories were not always cited as actual data collected. Sometimes they were mentioned as data they may want to have access to. Globally, employees in our sample of participants had a precise idea of data collected in their company. We can however note that the precise idea they have is equivalent to the official employer sayings about the data collected. This questions the theme of trust presented later on, in 7.4. The first category is the personal identity data: ID card or contact information, for example. The second is the wage-linked data: bank details, wage or family situation, for instance. The third category is the operational data: working hours, hourly efficiency or breaks timing. In most firms, this is the kind of data that is mainly used by and for human resources (HR) [20]. Accordingly to this, one participant asserted "I trust my employer [concerning data privacy], but if I had to doubt, I would doubt the HR department. They are those for whom data is the most beneficial" (P5). Finally, the fourth corresponds to the working data: employee career, employee expertise or working documents collected as documents and stored on enterprise-specific cloud platforms. The working documents stored are then accessible by the working team or by the precise working position of the employees. These two last categories are those on which focuses Inverse Transparency research [9]. In fact, they represent data that have value for other employees to know, one participant mentioned "I don't care having the name or the family situation of another employee. However, having the expertise domain of a new team member who will join us would be helpful" (P9).

Private Life When participants were asked about the type of data that was collected, the answers were vague. In fact, a lot of participants (P2, P3, P5, P6) responded close to: "I know that my data is collected everywhere on the web but I cannot name precise data types besides my name, e-mail address or phone number" (P4). More interestingly, most of the participants were unable to explain where and how their data is collected: "I know that my data is collected because I see a correlation between my Google search and the advertisements I see. I do not know how this is collected or where this is stored" (P8). Moreover, this is the starting point of the *Usable Privacy Policies Project* [21].

Comparison We note that the most valued data categories by employees, operational and working data, are those that are more workplace-specific. Therefore, when considering the concept of Inverse Transparency outside of the workplace, the motivation change. In both environments, the participants often stated that they have not a precise idea of what data is collected: "it's hard to make an exhaustive list" (P4), "the web environment is too complex" (P7). However, when comparing the answers, more vagueness was observed in private life. Besides, participants were able to justify the collection of their data in the workplace, for example, bank details are needed for wage payment: "My employer has my bank account details but this is needed for wage" (P5). The justification is expressed beginning with *but*. This was not true in the private life context.

7.2 Power balance

Workplace As stated earlier, a first key element in Inverse Transparency towards limiting data misuse is power balance. In the workplace, the employer strongly holds the power balance [4]. A clear contract ties together the employer and the employee: the employer pays employees for the work they are doing. When asking the participants, the power balance is not important regarding data privacy when the interests of the employer and of the employee are the same. In short, when there

is no litigation. This is also important to note that in the workplace, there is often a complex hierarchy structure. Therefore, the data-based control can be exercised on multiple hierarchical levels. The power balance is then to consider between different pairs within the enterprise: employer-employee but also manager (employer representation) - employee. In fact, in global companies, senior managers have control over project managers who control team members and HR control group of employees. [22]

Private Life The contract between the data provider and the data user was not so explicit in the mind of the participants. When visiting a website, the contract is the privacy policy. Therefore, these changes across websites and according to our survey privacy policies are opaque to website's users. All of our participants answered that they never read privacy policies. Privacy policies are too complex and thus impractical for consumers, and one criterion that could help them is standardization. [23]
Another expression of power balance that arises in the private life domain is loyalty. On the one hand, the data user wants data providers to come on the website. On the other hand, the data provider comes to the website to access a service.

Comparison The power relation exists in both environments. In the workplace, the power balance is between the employee and several hierarchy level. In private life, the power balance is often correlated to loyalty to a website, and we will address this point in 7.4. The contract between the data provider and the data user is well defined in the workplace whereas in private life, where contracts are too complex for most of data providers to understand.

7.3 Data privacy concerns

Workplace Participants did not express concerns about their data privacy towards their employer. They evaluated the data collected by their employer as limited. Some data is seen as necessary, for instance, bank account details are needed for wage payment. Operational data is the type of data that collection was the more mitigated among our participants' sample. Concerning the working hours, one participant stated "this is normal for my employer to check if I work accordingly with my contract" (P3), others argued "We are in a relationship of trust with my employer, if he wants to oversee my working hours, he breaks the trust, and I will no more work in the same constructive way" (P1). In fact, the default position of an employee is against workplace surveillance while the default position of an employer is for workplace surveillance [4]. In addition, even though they did not want their data to be seen by other employees, they are confident that their employer stores their data in a secure manner: "I had to install Stormshield during my first day at work, they pay attention to our data protection, this could be very problematic for them if there were a data breach" (P6). Consequently, participants did not report on using something to limit their professional data at work.

Private Life In our survey, a positive correlation appears between the awareness of individuals on data privacy issues and their willingness to keep their data private. The complexity of the web environment and the vast amount of data potentially collected are a first reason for individuals not willing to look at their data collection. In our survey, six participants expressed their data privacy concerns. As the willingness of individuals to keep their data private is limited to a part of the population, the willingness of individuals to use TETs and PETs vary. In fact, there are a lot of ideas and tools available today to protect individual data privacy. However, some categories of tools are not known or don't attract users. [15]. In our survey, all participants used at least one Google application. However, only one of them did already went to the Google dashboard. According to Google, "The Google Dashboard allows you to view and control data associated with the different products you use with your Google Account". After reading this description to the participants of the survey, some were not interested at all in this tool and others were interested by "pure curiosity" (P6, P7, P10) or "punctual dashboard visit" (P5, P8). This highlights two barriers before the use of TETs or PETs: the *knowledge* of the existence of these tools and the *attractiveness* of these tools.
Data users (companies) often share personal data in exchange for money and participants were aware of that: "If it's free, you are the product" [4] (P9). In fact, as mentioned by some participants, one can exchange money for more privacy, "LinkedIn Premium offers both to view who has seen my profile while staying in the private mode. Without premium, one has to choose between one of them" (P10). Like some free cookies options, LinkedIn Premium is a chargeable option. The link between money and data is here direct. We see here, that the interest of the data provider (free internet and data privacy) and of the data user (huge amount of data to earn money) is then opposed.

Comparison According to our survey, while some of the participants where concerned about their data privacy in private life, this was no longer the case in the workplace. This is here a clear difference. This difference is also linked to the trust component. In addition, the interests for data privacy of the data provider and of the data user appear to be more distinct in private life than in the workplace.

[4] Well known expression, following the idea of Richard Serra et Carlota Fay Schoolman (1973), Tom Johnson (2001), and Andrew Lewis (2010)

7.4 Trust and Loyalty

First of all, trust is related to the perception one's has of the environment [10] and to the level of one's data privacy concerns. Therefore, for the same parameters, two individuals may have a different level of trust. We noticed it during our interviews. In this section, we directly compare the answers for the workplace and for private life.

The parameters determining trust differ when looking at the workplace or when looking at private life. In the workplace, trust is based on the employer-employee relationship and stressed by the legal framework: one participant asserted "I believe that my employer follows legal rules" (P2). This assertion was common to all our participants working in big companies. Trust was common to all the participants in our sample. In private life, participants mentioned two main parameters: the service provider and the way information is displayed. The service provider parameter corresponds to the brand image, the brand nationality and brand fame. Two participants stated "I trust the GAFAM [5]" (P10) but others stressed "My personal data is too much collected, in particular by the GAFAM" (P5). This highlights again the subjectivity of trust.
According to our survey, the level of data privacy concerns plays also a role in trust. In the workplace, as we have seen in 7.3, participants did not mentioned data privacy concerns in the workplace. Consequently, one participant answered: "I trust my employer and anyway my personal data they have is not sensible" (P6). In private life, data privacy concerns are more expressed and the trust was not a ground truth, "I don't believe that disabling Cookies or adjust parameters change the fact that my personal data is collected" (P6). In our survey, we observed that the perceived opacity (and then transparency) influences the level of trust. Awad and Krishnan also establish a link between transparency, trust, and loyalty.

The presence of trust has different implications in the workplace and in private life. While in the workplace, absence of trust implies ineffective working and loss of time [9], in private life absence of trust imply product and use adjustment. While in the first case employers have an effective workforce to lose, in the second case firms' products may lose market share. In the end, this comes to a common loss of attractivity. Different factors are to consider when talking about service loyalty. In fact, service loyalty is linked to trust [10] but equally important to service value [24]. In our survey, parameters such as uniqueness or rapidity were cited by participants as parameters which bypass their sentiment of untrustworthy environment. If they consider a service to be unique, they use it even though they do not trust it completely.

[5]The well-known GAFAM for Google Amazon Facebook Apple Microsoft but now more precisely GAMAM for Google Amazon Meta Apple Microsoft

These links between trust, loyalty, data privacy concerns, and service value are summarized in Figure 3. As mentioned in 7.2, loyalty can be seen as a power balance. The power balance is between the level of trust and the service value, concerning website's cookies one participant answered "it depends on the level of trust I have on the website and on the service it offers. For example, if the service is confidential I disable cookies and use private browsing" (P1). This was expressed as a trade-off by some participants: "I am ready to share my data in exchange for a quality service. I think that personalisation is a win-win tool for both individuals and companies" (P3). We are back on the trade-off between data based innovations and data privacy [8].

7.5 Display

We have seen that a large amount of data is collected both in the workplace and in private life. Consequently, a person cannot oversee entirely its data processed easily [1]. This comes with a challenge: how to display information in order to have control over personal data? In both environments, keywords among our participants were "consistency", "centralization" and "standardization". In the workplace, consistency and standardization were mentioned by participants in a perspective of efficiency and rapidity: "The consistency effort for project report made by my company two years ago is helpful to find the information needed quickly" (P2). This goes with templates for each process stage, which is more and more used by companies according to our participants. In the private life, one participant stated "I have a lot of loyalty cards and different access for each of them, it is impossible to check each. I would like to have a single access for all, with centralized information" (P8). There is a single company involved in the workplace, the one for which you work, whereas, in private life, the actors are numerous.

7.6 Technical scalability

Some insights into the technical challenges raised by Inverse Transparency are given by our survey. However, no technical questions were asked to participants.

Workplace All employees work on the same intranet or relatively closed numerical environment. In addition, the data user (employer) is quite unique. The data stays in one company, the one the employee has a contract with. Finally, due to professional secrets and companies competitions, employers are likely to want the working data of their employees to stay private. There is a common interest of the employer and of the employee for data privacy outside of work. The numerical environment is closed also in that way.

Private life Data is created in a lot of different tools and platforms, and the companies involved are numerous. This

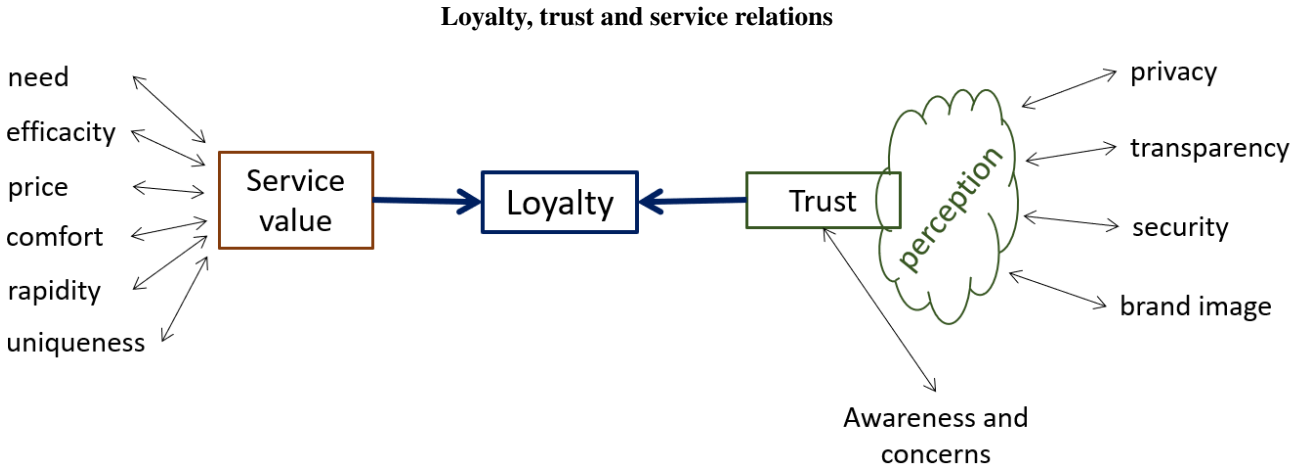

Figure 3: This graph presents the relation between consumer loyalty (middle), consumer trust (right) and service value (left) for the consumer, and major components that influence these three concepts. It emphasis the subjective character of trust which appear to be a *perceived* trust. This graph is based on our participants' answers and on [10, 24]

.

leads to heterogeneous privacy policies, goals and displays. Based on our survey, participants believe that the data collected represent more kinds of personal information than in the workplace. In brief, numerical environments are open, much more than the company's intranet.

Comparison Therefore, the TETs may be more difficult to develop and scale up in this second environment. Inverse Transparency framework should be integrated into all apps and systems to be usable: this is feasible for one company intranet but not for the entire web [1]. We come back on the four mainstay components of Inverse Transparency presented before and present them regarding private life. (A) *Data usage track*: More data to track with increased room for out of Inverse Transparency system data collection. (B) *Authentication and data usage's storage*: Storage of a large amount of data and authentication of all data users (companies, websites, apps, devices). (C) *Display collected information*: centralization of information detained by multiple companies and consequences expected on the data market. (D) *Data management*: Plenty of tools already exists in this category and each tool involves a limited number of service provider. That goes against the wishes of participants for centralization. In addition, the large amount of data processing, storage and tracking brings environmental challenges [25] and technological challenges [26]. It appears that from a technical point of view, the challenge is not of the same scale for the workplace or for private life.

8 Conclusion

First, it is important to note that our approach is only qualitative and not quantitative. We can highlight tendencies but we cannot deduct generalizations. As we have seen, persons have their own sensibility, knowledge, and perception of their data privacy. In addition, for the same level of awareness, several persons may have different practices (theory and practices are not always consistent). In brief, each user has unique online practices. Our qualitative approach highlighted these discrepancies.

The main purpose of this paper was to synthesize and taxonomize the concept of Inverse Transparency along with transparency-enhancing tools, privacy-enhancing tools, and privacy. Three graphs were also created in this summarization perspective. A survey was organized to access the usefulness and scalability of the concept into the private life domain. According to that, we described the concept of Inverse Transparency and the four main categories of components on which it relies. In these categories, there are an endless number of TETs and even PETs that help address some types of technical challenges raised by Inverse Transparency. However, most of these tools are not widely used. The concept, thought for the workplace, appears to tackle several trade-offs [1, 2, 9]. Therefore, we explored its scalability in private life. For this purpose, we used a qualitative survey approach with one-to-one semi-structured interviews asking open-ended questions. We then used a thematic analysis approach to analyze the data collected during interviews. This survey's purpose was to highlight the difference that arises when considering data privacy and Inverse Transparency at work or in private life. It appears that the scale of data collected is not the same, and much more bigger in private life. Participants were more concerned by their data privacy in their private life. Therefore data tracking tools make more sense for them in their private life, the interest of participants in such tools was high. However, the already existing tools do not attract many users. This gap may be to consider and more importantly to understand

in future work. For instance, is it due to education or to an irretrievable gap between theory and knowledge. The critical point towards achieving the scalability of Inverse Transparency into the private life is the technical scalability. As mentioned above, this is unfeasible today. However, technological improvements are fast and what is unfeasible today may be feasible in the future. Another point is that the interest of the data provider and of the data user can be opposed in private life. The motivation of each side is therefore to address in future work.

References

[1] Valentin Zieglmeier and Alexander Pretschner. Trustworthy transparency by design. *CoRR*, abs/2103.10769, 2021. https://arxiv.org/pdf/2103.10769.pdf.

[2] Andreas Boes. Inverse transparenz, beteiligungsorientierte ansätze für datensouveränität in der digitalen arbeitswelt gestalten. https://www.inversetransparenz.de/, (accessed on 13 November 2021).

[3] Oana Brindusa Albu and Mikkel Flyverbom. Organizational transparency: Conceptualizations, conditions, and consequences. *Business Society*, 58(2):268–297, 2019. https://doi.org/10.1177/0007650316659851.

[4] Lucas D. Introna. Workplace surveillance, privacy and distributive justice. *SIGCAS Comput. Soc.*, 30(4):33–39, 2000. doi: 10.1145/572260.572267. https://doi.org/10.1145/572260.572267.

[5] Carmen Mayer. Data-based transparency and leadership in small and medium-sized enterprises. In *SKILL 2021*, pages 39–50. Gesellschaft für Informatik, Bonn, 2021. https://dl.gi.de/bitstream/handle/20.500.12116/37780/A2-1.pdf?sequence=1&isAllowed=y.

[6] Tobias Pulls. *Privacy-Preserving Transparency-Enhancing Tools*. Faculty Of Economic Sciences, Communication And It, Computer Science, Karlstads Universitet, 2012. https://www.diva-portal.org/smash/get/diva2:570706/FULLTEXT01.pdf.

[7] Marijn Janssen and Jeroen van den Hoven. Big and open linked data (bold) in government: A challenge to transparency and privacy? *Government Information Quarterly*, 32(4):363–368, 2015. https://doi.org/10.1016/j.giq.2015.11.007.

[8] Andrew Trask, Emma Bluemke, Ben Garfinkel, Claudia Ghezzou Cuervas-Mons, and Allan Dafoe. Beyond privacy trade-offs with structured transparency. *CoRR*, abs/2012.08347, 2020. https://arxiv.org/abs/2012.08347.

[9] Maren Gierlich-Joas, Thomas Hess, and Rahild Neuburger. More self-organization, more control-or even both? inverse transparency as a digital leadership concept. *Business Research*, 13, 2020. https://doi.org/10.1007/s40685-020-00130-0.

[10] Carlos Flavian and Miguel Guinalíu. Consumer trust, perceived security and privacy policy: Three basic elements of loyalty to a web site. *Industrial Management and Data Systems*, 106:601–620, 2006. https://doi.org/10.1108/02635570610666403.

[11] Peter Dabrock. From data protection to data sovereignty. a multidimensional governance approach for shaping informational freedom in the 'onlife'-era. *Cursor Zeitschrift für explorative Theologie*, 2019. https://doi.org/10.21428/fb61f6aa.f0bf0cc2.

[12] Stefan Schmalz, Carmen Ludwig, and Edward Webster. The power resources approach: Developments and challenges. *Global Labour Journal*, 9(2), 2018. https://doi.org/10.15173/glj.v9i2.3569.

[13] Mena Teebken and Thomas Hess. Privacy in a digitized workplace: Towards an understanding of employee privacy concerns. In *54th Hawaii International Conference on System Sciences*, 2021. https://doi.org/10.24251/HICSS.2021.800.

[14] Dayana Spagnuelo, Ana Ferreira, and Gabriele Lenzini. *Transparency Enhancing Tools and the GDPR: Do They Match?*, pages 162–185. 2020. https://doi.org/10.1007/978-3-030-49443-8_8.

[15] Office of the Privacy Commissioner of Canada. Privacy enhancing technologies – a review of tools and techniques, 2017. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/#heading-0-0-15, (accessed on 28 December 2021).

[16] Hans Hedbom. A survey on transparency tools for enhancing privacy. In *IFIP Summer School on the Future of Identity in the Information Society*, pages 67–82. Springer, 2008. https://dl.ifip.org/db/conf/ifip9-6/fidis2008/Hedbom08.pdf.

[17] Alessandro Oltramari, Dhivya Piraviperumal, Florian Schaub, Shomir Wilson, Sushain Cherivirala, Thomas Norton, N.Cameron Russell, Peter Story, Joel Reidenberg, and Norman Sadeh. Privonto: A semantic framework for the analysis of privacy policies. *Semantic Web*, 9:1–19, 2017. https://doi.org/10.3233/SW-170283.

[18] Adi Bhat. Qualitative research: Definition, types, methods and examples, 2018. https://www.questionpro.

com/blog/qualitative-research-methods/, (accessed on 11 January 2022).

[19] Ditte Mortensen. How to do a thematic analysis of user interviews, 2019. https://www.interaction-design.org/literature/article/how-to-do-a-thematic-analysis-of-user-interviews, (accessed on 15 January 2022).

[20] Maren Gierlich-Joas and Thomas Hess. Towards an understanding of data's influence on leadership. In *15th International Conference on Wirtschaftsinformatik*, 2020. https:/doi.org/10.30844/wi_2020_q3-gierlich.

[21] Norman Sadeh. Usable privacy policy project, 2019. https://www.usableprivacy.org/, (accessed on 9 January 2022).

[22] Jakob Heumann, Martin Wiener, Ulrich Remus, and Magnus Mähring. To coerce or to enable? exercising formal control in a large information systems project. *Journal of Information Technology*, 30(4):337–351, 2015. https://doi.org/10.1057/jit.2014.11.

[23] Joel R. Reidenberg, N. Cameron Russell, Vlad Herta, William Sierra-Pambley, and Thomas Norton. Trustworthy privacy indicators: Grades, labels, certifications and dashboards. *Washington University Law Review*, 96(6), 2019. https://ssrn.com/abstract=3342747.

[24] Naveen Farag Awad and M. S. Krishnan. The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, 30(1): 13–28, 2006. https://doi.org/10.2307/25148715.

[25] Miyuru Dayarathna, Yonggang Wen, and Rui Fan. Data center energy consumption modeling: A survey. *IEEE Communications Surveys Tutorials*, 18(1):732–794, 2016. https://doi.org/10.1109/COMST.2015.2481183.

[26] Rajeev Agrawal and Christopher Nyamful. Challenges of big data storage and management. *Global Journal of Information Technology*, 6, 2016. https://doi.org/10.18844/gjit.v6i1.383.