I Trust You Dr. Researcher, but not the Company that Handles My Data – Trust in the Data Economy

Rebekah Rousi
University of Vaasa
Rebekah.rousi@uwasa.fi

Joni-Roy Piispanen
University of Vaasa
joni-roy.piispanen@uwasa.fi

Jani Boutellier
University of Vaasa
jani.boutellier@uwasa.fi

Abstract

In the rising era of artificial intelligence (AI), learning machinery and hyper surveillance, trust is a sought-after attribute. The General Data Protection Regulation (GDPR) was introduced to increase individuals' control over their own personal data, yet proof of its effectiveness is still lacking. Contrary to the agenda of the GDPR, recent studies have shown numerous flaws in the regulation including user negligence and ignorance, to manipulation via dark design patterns. Even though informed via compulsory privacy notices, people still experience less trust than ever. This impacts every area of human society. This paper reports two interview studies (N=31) that probed individuals' trust towards company-driven data handling practice and communication. The results demonstrate low to no trust in the perception of data-related information given by companies. Participants perceived researchers as more trustworthy regarding data-handling related communication and practice.

Keywords: Trust, Data Privacy, Communication, General Data Protection Regulation (GDPR), Business, Video Surveillance

1. Introduction

According to Rachel Botsman (2017), trust is fast becoming the commodity of the 21st century. In fact, every transaction relies on trust (Robbins, 2016). This holds for technology use as much as for commercial transactions. Throughout human history, people have developed technology upon which they become reliant. Knives, axes, hammers, paints. While back in prehistoric days there was a primal relationship between humans, form and function of the developed tools, these days the relationship has become radically abstract and complex. Several decades ago, humans riding in an elevator trusted the vehicle's physical mechanics for its reliability in delivering their body (and mind) safely and smoothly from one height to another (Rousi, 2014). These days elevators are not simply boxes with a motor and electronic controls, but rather a system of systems in which the physical mechanics is one portion of the data-driven system that connects with services and more systems, to transport people from one floor to the next. In other words, human-technology interaction (HTI) relationships have transformed from trust between person and object, or person and object's developer/designer (see e.g., Saariluoma & Rousi, 2015), to trust between person and mass-amounts of faceless counterparts – code (software programs), people, components (hardware etc.). Moreover, inside many of these elevators as with any type of urban environment (interior and exterior), are surveillance cameras and other sensory technology.

HTI has been transformed from a human-utilization relationship, to a human-surveillance interaction. The walls and ceilings have eyes and ears. Where regulations such as the General Data Protection Regulation (GDPR) are intended to increase the control of citizens over their personal data, situations in which people have no control over opting in or opting out of data collection are on the rise (Geradin, Karanikioti & Katsifis, 2021). While all environments are bugged, all services are digitized. Records, transactions, preferences, habits are all stored in cyber space – and they are worth profit (Winegar, & Sunstein, 2019). There are significant developments in areas of information technology (IT), particularly artificial intelligence (AI), intended to improve life quality and wellbeing (Holzinger et al., 2023). Yet, all of these machine learning (ML) systems rely on the collection of data – personal and otherwise – to learn, adapt and respond to specific conditions and situations (Liu et al., 2021). This makes AI development and implementation a shady area for ethical discussion. For, no matter what the intention behind the technological development, the collection and utilization of personal data will always pose challenges from one direction to another, none-the-least general privacy debates and experiences (Liu et al., 2021). Populations are becoming aware of the commercial value, exploitation and manipulation of their personal data (Barth et al., 2019).

This paper focuses on reporting portions of two studies: 1) the experience of AI-enabled anonymized

URI: https://hdl.handle.net/10125/106941
978-0-9981331-7-1

video surveillance for assisted living; and 2) 'at-work' surveillance to detect issues related to wellbeing. The authors concentrate on the matter of corporate trust in relation to personal data collection and data handling.

2. Trust and data

Trust is a heavily contested concept that has its scholarly roots in sociology and psychology (Cook & Santana, 2020). From a sociological perspective, trust arises in social life through relations, encounters and experiences (Robbins, 2016). Trust enables cooperation and lowers the threshold for engaging in interactions and forming relationships (Robbins, 2016). Trust is the belief that if one engages in interaction or utilization of something, or allows another individual, being or device to act on one's behalf, the outcome will be that which is intended (McLeod, 2021). There are various theories of trust from risk-assessment theories (Jones, 1999) to end-directed rationality (Baker, 1987). Discussions have also focused on rational trust versus irrational trust (Saariluoma, Karvonen & Rousi, 2019) – rational trust being an evidence-based belief that a trustor can rely on a trustee to successfully deliver a given action or proposition, and irrational trust connecting to virtue. Virtue in this case exists within qualities of the trustee, e.g., brand, aesthetic properties, familiarity and resonance (McLeod, 2021).

Trust in its raw sense goes beyond pure belief (Hieronymi, 2008) and towards a psycho-physiological state that either enables or prevents individuals from allowing others (people, beings, objects or systems) to operate on their behalf (Ajenaghughrure, Sousa, Kosunen & Lamas, 2019). Properties and qualities of the trustee are important (McLeod, 2021). Thus, either explicitly (consciously) or implicitly (subconsciously) risk-assessment is undertaken when engaging in transactions and interactions (Jones, 1999). There has been critique against risk-assessment theories for instance, as they do not distinguish between trust and reliance (Jones, 1999). In the context of this paper, the authors apply trust to the understanding that there are various chronological phases in HTI that activate various forms of trust, from the willingness to engage in certain types of technology (Saariluoma et al., 2019) to reliance on the technology. When thinking of an elevator for instance, failure to trust would either result in anxiety during elevator travel or reluctance to board the elevator in the first place.

Samir Passi and Steven Jackson (2018) focus on the ways in which trust is operationalized within the field of data science. They draw on the sociology of science to observe the constructs of trust and credibility in relation to scientific method, process and output. The origins of scientific trust stemmed from a social perception in which 'gentlemen' were viewed as "reliable truth-tellers" (Shapin, 1994). This is interesting from the perspective of corporate trust due to the role of marketing and 'story-telling' in establishing, building and sustaining trust (see e.g., Langer & Thorup, 2006; Huoang & Guo, 2021). The gentlemen Shapin (1994) and Shapin and Shaffer (1985) speak of were males born of noble birth. Thus, blood and upbringing bound them to an image of righteousness, virtue, and honor. This instilled integrity and credibility through authenticity of who the individuals were by birthright. Passi and Jackson (2018) state, "data science is a sociomaterial practice (Orlikowski, 2007) in which human and technical forms of work intertwine in specific, significant, and mutually shaping ways" (p. 136:2). Enabling data-based trust, both in science as well as in other organizational contexts involves action and practice that is embedded with firm conventions and governance (Passi & Jackson, 2018). A large part of these conventions involves the communication used between organizations and the populations from whom they are collecting data.

The GDPR is a measure that has been designed and implemented to strengthen trust between individuals, systems, and organizations through increasing levels of awareness regarding how personal data is being collected, what types of data are collected, how they are being used and stored, and indeed, through requiring consent on behalf of Internet users (Greengard, 2018). However, the effectiveness of the regulation has been fraught with controversy, focusing on the quality of communication and acceptance protocols (cookie notices) that often entail a lack of understanding of legal jargon (Santos et al., 2021), failure to read extensive texts (convenience) (Liao et al., 2020), and peer-pressure (fear of missing out – FOMO; privacy paradox) (Tandon et al., 2021) that see individuals compromise their privacy and/or blindly accept the acquisition of cookies.

3. Organizations and [anti]trust

The world of Big Tech is characterized by its role in the data-driven surveillance economy (Kenney & Zysman, 2020). A combination of many factors has contributed to a lack of trust in large technology companies, none-the-least, the ways in which they collect and use the personal data of users. As ironically stated by Richard Serra (1973), "if the product is free, then you are the product." The original quote was made in the context of a short film *Television Delivers People* – a critique against mass media and its position as a social construct reinforcing control over populations. We see here the pre-emergence of what is currently faced in the data economy. Individuals are trapped in the

privacy paradox as a mixture of FOMO (Abel, Buff & Bun, 2016) as well as social and economic exclusion – often represented in digital divide discussions (see e.g., Lynthreatis, Singh & ElKassar, 2022).

A clear challenge is that the Internet and emerging AI systems are not democratic or equitable. Rather, they are vehicles to expedite monopolization through business models that run on digital platforms (platform economy; Kenney & Zysman, 2020) to which all contribute, yet few have access (Armoogum, Davies & Mariuzzo, 2022). There are not only high set up costs, but expensive maintenance and updating costs, making existence difficult for smaller players (Prasanna et al., 2019). Yet, once up and running, Big Tech companies that act like platforms have low to zero marginal costs (Armoogum et al., 2022). Due to the networked global nature of the Internet, they scope and scale-up rapidly.

The persistent ethical challenge of these Big Tech companies is the ways in which they exploit customers. It is not only the people who 'play for free' who are subject to being *the product*, but also those increasingly pouring in money for services (Birch, Chiapetta & Artyushina, 2020). All of these factors affect the ways in which people approach and understand privacy and ethical issues in relation to organizations, and commercially-driven corporations. Big Tech sells data to advertisers and counterparts making personal data the oil of the 21st century (Nolin, 2020). With an underestimation on the value of trust there is a severe overlooking of the consequences for future technological development (Toulouse et al., 2020).

4. Method

The two studies reported in this paper both employed interviews. Study 1 followed a structured interview format, while Study 2 was designed in semi-structured format. Both studies focused on different aspects of privacy in two use contexts. Study 1 aimed at observing the experience of AI-enabled anonymized video surveillance that captures and recognizes movement and behavior without disclosing people's identities. The use context for the study in question was the home from the perspective of assisted living. Study 2 was based on retrospective interviews with researchers and participants of a research project that examined the use of sensory technology to enhance workplace wellbeing. Study 2 focused on the experiences of privacy by researchers and participants regarding workspaces fitted with cameras and keystroke trackers. This paper focuses on reporting the results of questions related to organizational trust in data handling.

4.1 Ethics

Researchers or both studies strictly followed the ethical guidelines of their research institutions, as well as research with integrity, specified by the Finnish National Board on Research Integrity (TENK). Moreover, GDPR was followed via issuing all potential recruitees with a research information notification, privacy protection notice, and informed consent form – which was signed before commencing the studies.

4.2 Study 1

The interviews of Study 1 took place onsite at a laboratory for human-computer interaction (HCI) research. Two researchers performed the interviews with one participant at a time. The study was multidisciplinary in that the researchers represented HCI, cognitive science, and communication studies, as well as software engineering, and machine learning. One researcher focused on the HCI components of the study, while the other focused on implementing the anonymized AI-driven video system and machine learning aspects of that system. Both interviewers conducted the interviews.

4.2.1 Participants

Participants were recruited via university emailing lists, Teams channels, and via snowball method. The data represents a convenience sample (Etikan, Musa & Alkassim, 2016) in order to allow for data-emergent insight on factors that will form the foundations of a model on privacy experience that will be validated via purposive sampling (Etikan et al., 2016) in future studies. Twenty participants were recruited for the study (7 female and 13 male). Ages ranged from 18 to 55+. The largest age bracket being that of 26-35 years of age.

4.2.2 Procedure

After ensuring that all GDPR procedures were completed, researchers first explained the procedure and components of the study. The study was also briefly presented once more in the context of the respective projects of the researchers. Facets of the HCI lab environment were shown, and instructions were given for actions participants were to undertake during the course of the experiment. Participants were asked to complete a background questionnaire hosted by Webropol, the online survey software. Upon completing the background questionnaire, participants were asked to perform basic actions, recognizable by the AI-driven action recognition system, in front of a camera. The actions were: sweeping the floor; watering a flower; eating; sneezing; and reading a newspaper. The video

experience part of the study comprised questions relating to: how comfortable the participants were with different versions of video - whether they preferred very low resolution (32x32 pixels, unidentifiable) footage or high definition (identifiable) of themselves; how people (visitors) should be notified if these systems were in domestic spaces; overall understandings of privacy; and whether or not the participants would trust a company that stated their system would not share any identifiable data from the resident's property (all data stored and processed in-device). The present paper focuses on reporting the findings of this final question – whether the participants would trust a company stating that it would not share personal data.

4.2.3 Analysis

Thematic analysis (TA; Clarke, Braun & Hayfield, 2015) was utilized as a flexible and lightweight means of categorizing explanations applied to justifying why participants either would or would not trust a company's data-handling communication. Due to the more concise sample size, the data was analyzed in Excel and is presented in graphs according to the amount of times a certain theme was mentioned.

4.3 Study 2

Semi-structured interviews were employed to probe the experiences of the participants in the former sensory technology and work wellbeing research project. The order of questions was dynamic, allowing for flexibility and adaptation according to each interviews flow. This methodology was chosen for the additional benefit of allowing the interviewer to shape the interviews according to the pre-interview survey. Thus, depending on the interviewee's role and knowledge of the project, the interviews were steered towards questions that might result in meaningful answers. To facilitate for a fluid interviewee experience, the interview structure contained questions, that were ordered according to thematic cohesion. Each thematically connected cluster of questions was connected to other clusters to provide multiple springboards for cases in which the interviewee's answer veered into other thematic directions. Separate interview structures were formed for researchers of the project and research participants.

4.3.1 Participants

Participants were contacted and recruited via the principal investigator (PI) of the former project. In order to recruit from a people pool attached to a prior project in an ethical and responsible way, the PI and a project manager identified potential participants and contacted the candidates to ask for consent in advance. This already gave a concrete indication of who would be willing to participate in the current study. Eleven participants took part in Study 2. Nine of the interviewees were test subjects of the project in question. This meant that while the project ran, these individuals were in situations in which their work environments were fitted with sensors. The work environments ranged from academic and industrial research environments to health and social care settings (back office). Two of Study 2's participants were researchers employed by the project. These were the people responsible for implementing, analyzing and reporting the activities of the project. Four participants were female and seven male. Ages ranged 25-64, The largest age bracket was 45-54.

4.3.2 Procedure

The interviews were conducted between March and May 2023. Each interview lasted from 20 to 120 minutes. The majority of the interviews lasted approximately 25 to 40 minutes. The researcher interviews were outliers, as the interviewees played significant roles in the project. Thus, the interviewees in question were able to elaborate on most answers, going deeply into the project details and their experiences. The interviews took place remotely via Zoom. The research subjects were asked via email to sign a consent form after reading the privacy notice and research notification. Once participants had consented, an interview time was arranged. Interviews were transcribed and translated by hand from Finnish into English.

4.3.3 Analysis

A lightweight narrative analysis (Franzosi, 1998) that examines the input of study participants who had served as participants in the research project in question, as compared to the statements given by project researchers was applied to the data of Study 2. The insights are contrasted with one another to form a comprehensive picture on the dynamics of participant experience versus researcher understanding.

5. Results

The results are reported here according to the study in question. Study 1 focuses on the responses to one question: *Would you trust a company who says they would not send data from this [anonymized video] device?* The results from Study 2 focus on the responses of three questions: Would you say that the relationship with those researchers had an impact; In what way would it have affected your experience, if some third-

party, for example a company or other entity was involved in collecting and processing your data?; and Could you elaborate on what else would have mitigated your concerns?

5.1 Study 1 Results

The distribution of positive (yes) and negative (no) responses to the question of whether or not participants would trust a company that assures they would store all data in-device was 60% (yes, 12) versus 40% (no, 8; see Fig. 1).

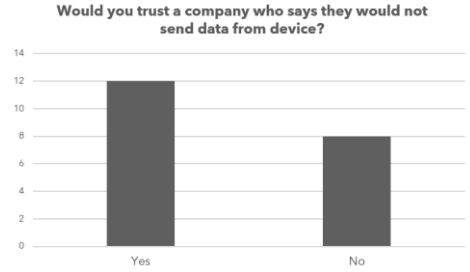

Figure 1. Yes and no responses to trust in a company that states it will store all data in-device.

Interestingly, there are no indications within the explanations to show that participants would 'blindly' trust a company based on words alone. Rather, a form of 'rational trust' (Saariluoma et al., 2019) is demonstrated, whereby information given by the company should be supported by further evidence. The explanation types (12 given in total) were as follows: validation/governance (8.3%); company reputation (25%); background research/ knowledge (41.6%); legal policies; transparency (8.3%); and benefits/good reasoning (8.3%) (see Fig. 2). Although not generalizable, these figures indicate that deeper understanding of the company and even transparency would assist in instilling trust.

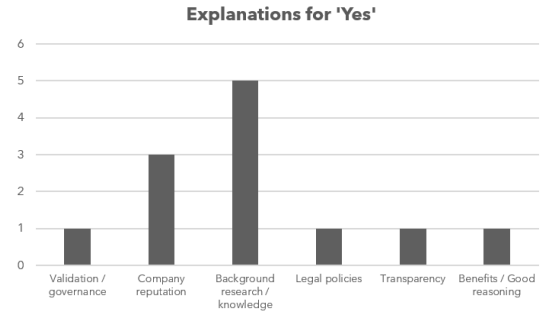

Figure 2. Explanations given for 'Yes'

In terms of validation and governance, one participant mentioned that the government should be involved in regulating the company in order to ensure that it acts appropriately. More people chose company reputation as a means by which they could trust. As one participant states,

> *"It certainly depends on the company. For instance, I wouldn't be so worried about you [as researchers]."* [P04, 07022023]

In this phrase, the participant expressed trust towards the researchers both as representatives of knowledge work (search for *truth*) in academia – understanding non-commercial intentions – as well as in terms of being familiar individuals. Background research or previous knowledge of the company in question was the most mentioned explanation,

> *"I would trust the company after performing good research on the company, or hearing stories about it from other people."* [P05, 07022023]

It seemed imperative to approach trust from a 'tried and tested' perspective, where not much in fact would be left to chance. The other explanations used related to legal policies (also connected to governance), transparency, whereby the operations of both the company itself and its products were fully explainable, with good reasoning about potential benefits – benefits outweighing the possible threats of the technology. Regarding the negative responses, two (25%) participants gave a flat "no" that they would not trust the company. Other explanations given were: home is a sensitive place (25%); unintended data collection (12.5%); Internet doesn't forget (25%); and I want to, but can't (12.5%) (see Fig. 3).

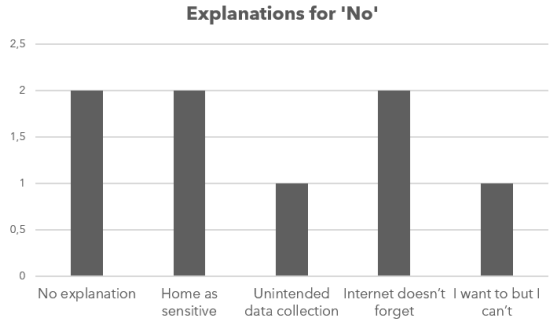

Figure 3. Explanations given for 'No'

Concern was made regarding the sensitive nature of the home. While participants could see that monitoring would be useful in the workplace, in the home participants did not want to take the risk of personal data leaks. Moreover, the issue of unintended data collection, or video surveillance capturing information that is either not relevant for the surveillance purpose and/or exceeds this purpose (i.e., highly sensitive information) was not seen as acceptable. Additionally, the lack of trust

towards corporate communication meant that two participants saw too great a risk in the data being leaked to the Internet,

> *"Anything you put on the Internet stays on the Internet forever… Maybe future generations are more comfortable with this."* [P06, 07022023]

Here, we observe generational reflections in terms of what would be and what would not be acceptable for people of diverse generations. There is an innate skepticism of the fact that the data could flow into the unforgetting space of the Internet. As another participant follows,

> *"[…] it would be simply a bonus […] then comes some data breach or something even worse. […] Or if it gets on the Internet, you can never fully trust the fact that the data will not be spread."* [P07, 07022023]

These concerns can be seen as linked to the last explanation that pertains to the fact that the participant would like to trust the company, its communication, and its system, but they cannot.

5.2 Study 2 Results

In Study 2 the researcher examined the dimensions of trust in relation to the data collecting and handling organization(s) participating in a project on sensory technology for increased work wellbeing. This was achieved by focusing on three questions pertaining to: 1) the relationship between the participants and the researchers; 2) how the potentiality of a third-party company collecting and handling data would affect their experience of trust; and 3) elaborating on responses and offering insight into mitigating concerns. The responses are divided according to the type of participant, i.e., the nine participants of the workplace wellbeing project in question, and the two project researchers carrying out the workplace wellbeing project.

5.2.1 Relationship to researchers and experience of privacy

Not all of the workplace wellbeing project participants of the study were directly familiar with the researchers working in the project. Yet, they were all indirectly familiar with the researchers on some level. On the basic level, the participants recognized the research organization coordinating and leading the project. On another level, some of the participants were connected to the project through contacts. While some of the participants (N=2) claimed that familiarity with the researchers did not play a role for various reasons – i.e., due to the study being conducted fully online, or due to general indifference – others emphasized a significant impact. As one participant explains,

> *"Would I have agreed to participate in something similar if it had been carried out by some research institute or entity, that I do not know? Perhaps not, or probably not. If we are talking about Finnish research institutes or universities, then I have a certain level of trust."* [P05, 042023]

Here, it may be observed that not only the organization itself, but its type and nationality are also key factors to instill trust. The reputation and codes of practice represented by particular countries are imperative to supporting organizational data trustworthiness. Another participant stipulates,

> *"If the data is handled by a large faceless corporation, human resources or management, then questions about the purposes, motivations and uses of the data arise. But knowing that this is for research purposes assures you about the ethical aspects […]."* [P10, 052023]

A similar strain of sentiment can be observed in the above quote as compared to those found in Study 1, noting that in addition to hesitation towards allowing big companies to engage in one's personal data, there was a genuine interest in understanding the benefits that the data collection could afford the individual. Also mentioned from the participants' perspective, was the quality of communication presented by the leading research organization. This quality comprised confidence and clarity in interaction, as well as direct correspondence between what was informed and how the research was operationalized. The researchers of the project emphasized measures taken in recruitment and procedure to ensure ethical practice. They described how external recruitment officers were used to eliminate peer pressure in the recruitment process, and explained about the conscious attention placed on language and communication to avoid coercive interaction with participants. Voluntariness was stressed from the perspective of the other researcher who stated that all were informed that the leading research organization was not the final data handler. Thus, a two-tiered approach to data trust can be seen in this study. The researcher maintained that this already tested participants' trust during the course of the project's study. Where participants were in doubt, they discontinued participation.

5.2.2 Effects of third-party data handling

All participants stated that having a third-party company handle the data of the research project would have affected the way in which they both trusted and engaged with the project. Six (66.7%) of the participants mentioned that they may have still participated in the project, but would have done so with caution – carefully reading all the details about the project as well as data collection and processing practices. Seven (77.7%) out of the nine former research project participants stated that nationality of the organization plays a key role in determining their trust in third-party data handling. Whether it was stating Finland directly as a trusted nation for data practices, or also neighboring countries and the European Union in general – particularly for their role in implementing and maintaining GDPR. The characteristic of the leading research organization in being a well-known Finnish research body was emphasized in contrast to commercially-driven entities. Once more, not all were disenchanted by companies being involved, for as one participant states,

> *"It depends on the company. I would have read the information regarding data processing much more carefully. […] For a large company, keeping the data safe within the research group and managing leaks are factors. For a smaller company, questions about their operational procedures, previous work, and connections, whether data is stored on dedicated servers […]* [P11, 052023]

Direct reference is made in the above statement to behavior adjustment and precautions that would be taken had a third-party company been involved in the data handling. There is also mention of the distinction between private and work life being more pronounced, as well as the differing circumstances that the participant would consider in instances where the company would either be large or small. Returning to the issue that a third-party was involved in the final data handling, the two researchers both articulated the crucial nature of the company in its role within the project. The company was utilized within the project for its capabilities in data privacy and security. They had performed security threat modelling and a security audit of the project's data practices. As one of the researchers mentions,

> *"The security threat modelling and external audit of the health monitor tool mainly emphasized the importance of these issues. […] In the case of the security audit, that was not about externalizing responsibility, but about avoiding sentiment contamination […]*" [P07, 042023]

Internal personnel recognized the necessity for acquiring extra capabilities and methodology from third-party sources. While national research organizations may represent qualities that embody trust for those participating in data collection, a part of maintaining this integrity is to recognize areas in which other organizations may have complimentary and/or advanced capacities to further reinforce the reliability and robustness of the data handling practices. One challenge however, as reflected in the attitudes of participants stated above, is the task of convincing decision-makers and legal experts of the need for third-party involvement. Communication was additionally articulated as a crucial factor in instilling and maintaining trust. In particular, communication in advance was seen as a key behavior that could boost transparency and support trust through increasing understanding as well as enhancing relationships between actors.

5.2.3 Elaboration and insight - mitigating concerns

There were many comments and suggestions that were placed by participants regarding either how concerns could be mitigated or why the project in question was a success. All nine participants from the former project emphasized the importance of clear, effective and systematic communication. As this participant states,

> *"[…] communication and informing are really important […] Being open about challenges and that some things don't work, lets us respond very quickly and react to those things. It's really important from a communication point of view. […] the fact that things are done as they were told to happen, schedules and so on."* [P05, 042023]

In addition to the ability to rely on information for its accuracy, emphasis was placed on the importance of availability, accessibility, and even openness in communication. While most participants experienced this openness, one participant stated that they would have felt more secure if they would have had the opportunity to engage in face-to-face discussion – both without computer mediation, as well as in a more relaxed and interactive way. The feeling of being able to access people. Another critical aspect to any type of data-driven project or initiative is careful and systematic documentation practices. Documentation in itself is connected to technical communication practice.

The two researchers involved in the project raised experiences and recounted mitigative action they actually engaged in. One of the researchers stated that they had to find solutions, thus requiring genuine and

open discussions within the project actors. Clear communication was once again named as the key ingredient to ensuring that everyone understood procedures and who to contact in case of doubt. This researcher also mentioned that some individuals who had originally been recruited for the study decided not to share their data. This matter was respected and the individuals were free to be excluded from the data collection. The other researcher elicited the vital nature of undertaking procedures that can be verified afterwards in terms of demonstrating how the data has been processed. They also mentioned,

> *"Openly explaining what are the concrete steps to take the matter forward. Make GDPR issues clear. Data destruction opportunity, etc."* [P08, 042023]

A great portion of ethical privacy preserving data handling relies on the quality, frequency, and accessibility of communication. The results of both studies reflect similarities between responses pertaining to communication, as well as to the importance of individuals possessing enough information, knowledge, and understanding to comprehensively understand the nature of both the data collection and handling as well as the organization(s) in question – their organizational culture (agenda), and nationality.

6. Discussion

There were some differences between the use contexts of the studies – one representing video surveillance and its experience in the home for assisted living, and the other probing the use of sensory technology to support wellbeing at work. Yet, issues arose within the data that supported an understanding of the ways in which people approach the matter of trust in organizations and organizational practice in data collection and handling. In both studies, participants emphasized the fact that they trusted the research organizations in question who were undertaking the studies. They trusted these research organizations on the basis of their familiarity, reputation, nationality (national regulations, principles, standards and practices), and perhaps mostly, the participants appreciated the aspect that through these organizations their data would not be exploited for profit. Thus, commercial goals seem to generate a conflict of interest within individuals. This poses an obstacle in relation to how people are capable of trusting company-delivered information related to data handling practices. Yet, as mentioned by one participant in relation to mitigating concerns, *organizational culture* plays a key role in trust. Organizational culture in itself is highly complex, and operates at different levels internal and external to the organization in question. It is however, the agenda and intention of the organizational leaders and management that embeds a sentiment through codes of practice and set work ethics that permeate through the culture of the organization.

Examples of dark design patterns for instance, are one indication or end-users that the values of a company are not in tune with discourse promoting fairness, sustainability and equity (Baker, 2020). Dark patterns in the form of difficulties to opt-out (comply or be punished), connecting to and utilizing personal data such as contacts and images, automatic credit card charges, and subscriptions that are difficult or near impossible to cancel, are reflections of both corporate strategy and organizational culture (Kim et al., 2023). These are immediate external signals that an organization cannot be trusted with one's personal data. Moreover, these organizations cannot be trusted near one's personal data. This affects not only trust in an individual company, but overall trust in the data-driven corporate ecosystem.

Nationality is another dimension to the organizational trust and data discussion. While the Internet spans international borders, nationality impacts trust more now than ever before. The GDPR seems to influence people's likelihood to trust data collection and processing. Therefore, organizations within the EU seemed more favorable in the responses of participants particularly in Study 2. The host nation of the study in question, and (research) organizations attached to this nation – Finland – held the highest credibility and trustworthiness, mainly based on familiarity with codes, procedures, regulations and standards. One nation in particular was raised numerous times, again in Study 2, as being an untrustworthy country.

7. Conclusion

The paper characterized the pertinence of privacy issues based on the experiences and vulnerabilities of existence in a data-driven society. It contributed to studies and discussions on the relationship between data privacy and corporate trust that is evidenced in recent research efforts (e.g., Huoang & Guo, 2021, and Passi & Jackson 2018). From the perspective of trust as a concept, we see from the results of both studies that participants never expressed a direct, intuitive or irrational trust (Saariluoma et al., 2019). Rather, all of their expressions of trust were justified through knowledge, background research and understanding of organizations who would potentially collect and handle their data. This sheds light on the matter of whether or not trust is in question at all. In Study 1 participants expressly stated disbelief that their data would not be shared via the Internet from the device.

The presented studies feature several limitations. The first relates to the small sample size of the studies. The studies give indications of how people may experience trust towards companies regarding their personal data, yet there are not enough participants to suppose generalizations or perform robust statistical analysis. Future research should concentrate on validating constructs emerging from the data via quantitative inquiry with a larger sample. Biometric measurements could be utilized to study physiological stress levels in domestic video surveillance and workplace 'sensing' experiments, and real-time think aloud (Jääskeläinen, 2010) or diary methods (Bolger, 2003) could be used to gauge qualitative experience. Moreover, the cultural dimension of data privacy and company trust is necessary to further examine (see Li et al., 2022; Raj et al., 2020; Saunders, 2012).

On the one hand, the economy should thrive on trust, given extreme competition between (smaller) players and human basic needs and motivations evolving around personal safety, security and wellbeing. The trouble being, as stated, monopolization is a key trait and threat of the data economy (Armoogum et al., 2022). On the other hand, as observed in current surveillance economy practice, individuals have fast learned that organizations and corporations cannot be trusted to be fair concerning data-driven practices. For this reason, measures such as GDPR have been introduced – to provide a scaffolding by which personal data, its collection, processing and mostly individual controlled, may be regulated (Greengard, 2018). The challenge is, that not only has GDPR served to heighten awareness and encourage agency on behalf of individuals, but GDPR itself has often been questioned for its effectiveness (Van Ooijen, & Vrabec, 2019).

Acknowledgements

The study was supported by the Research Council of Finland projects 345683 and 348391, University of Vaasa, Schools of Marketing & Communication, Technology & Innovation, Digital Economy, and the AI Forum project (Finnish Ministry of Culture & Education). We would like to thank Masud Fahim for implementing the human action recognition software.

12. References

Abel, J. P., Buff, C. L., & Burr, S. A. (2016). Social media and the fear of missing out: Scale development and assessment. *Journal of Business & Economics Research (JBER)*, 14(1), 33-44.

Armoogum, P., Davies, S., & Mariuzzo, F. (2022). The changing face of anti-trust in the world of Big Tech: Collusion versus Monopolisation. *Cambridge Journal of Economics*, 46(6), 1455-1479.

Ajenaghughrure, I. B., Sousa, S. C., Kosunen, I. J., & Lamas, D. (2019, November). Predictive model to assess user trust: a psycho-physiological approach. In *Proceedings of the 10th Indian conference on human-computer interaction* (pp. 1-10).

Baker, B.D. (2020) Sin and the Hacker Ethic: The Tragedy of Techno-Utopian Ideology in Cyberspace Business Cultures. *Journal of Religion and Business Ethics*, 4, 1. https://via.library.depaul.edu/jrbe/vol4/iss2/1

Baker, J. (1987). Trust and Rationality. *Pacific Philosophical Quarterly*, 68(1): 1-13. doi:10.1111/j.1468-0114.1987.tb00280.x

Barth, S., de Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*, 41, 55-69.

Birch, K., Chiappetta, M., & Artyushina, A. (2020). The problem of innovation in technoscientific capitalism: data rentiership and the policy implications of turning personal digital data into a private asset. *Policy studies*, 41(5), 468-487.

Bolger, N., Davis, A., & Rafaeli, E. (2003). Diary methods: Capturing life as it is lived. *Annual review of psychology*, *54*(1), 579-616.

Botsman, R. (2017). *Who can you trust?: how technology brought us together–and why it could drive us apart*. Penguin UK.

Clarke, V., Braun, V., & Hayfield, N. (2015). Thematic analysis. *Qualitative psychology: A practical guide to research methods*, 3, 222-248.

Cook, K. S., & Santana, J. J. (2020). Trust: perspectives in sociology. In *The Routledge Handbook of Trust and Philosophy* (pp. 189-204). Routledge.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American journal of theoretical and applied statistics*, 5(1), 1-4.

Franzosi, R. (1998). Narrative analysis—or why (and how) sociologists should be interested in narrative. *Annual review of sociology*, 24(1), 517-554.

Frenkel, A., Maital, S., Leck, E., & Israel, E. (2015). Demand-driven innovation: An integrative systems-based review of the literature. *International Journal of Innovation and Technology Management*, 12(02), 1550008.

Geradin, D., Karanikioti, T., & Katsifis, D. (2021). GDPR Myopia: how a well-intended regulation ended up favouring large online platforms-the case of ad tech. *European Competition Journal*, 17(1), 47-92.

Greengard, S. (2018). Weighing the impact of GDPR. *Communications of the ACM*, 61(11), 16-18.

Hieronymi, P. (2008). The Reasons of Trust. *Australasian Journal of Philosophy*, 86(2): 213–236. doi:10.1080/00048400801886496

Holzinger, A., Keiblinger, K., Holub, P., Zatloukal, K., & Müller, H. (2023). AI for life: Trends in artificial intelligence for biotechnology. *New Biotechnology*, 74, 16-24.

Huang, C., & Guo, R. (2021). The effect of a green brand story on perceived brand authenticity and brand trust: the role of narrative rhetoric. *Journal of Brand Management*, 28, 60-76.

Jones, K. 1999. "Second-Hand Moral Knowledge", *The Journal of Philosophy*, 96(2): 55–78. doi:10.2307/2564672

Jääskeläinen, R. (2010). Think-aloud protocol. *Handbook of translation studies*, *1*, 371-374.

Kenney, M., & Zysman, J. (2020). The platform economy: restructuring the space of capitalist accumulation. *Cambridge journal of regions, economy and society*, 13(1), 55-76.

Kevork, E. K., & Vrechopoulos, A. P. (2009). CRM literature: conceptual and functional insights by keyword analysis. *Marketing Intelligence & Planning*, 27(1), 48-85.

Kim, K. K., Kim, W. G., & Lee, M. (2023). Impact of dark patterns on consumers' perceived fairness and attitude: Moderating effects of types of dark patterns, social proof, and moral identity. *Tourism Management*, 98, 104763.

Langer, R., & Thorup, S. (2006). Building trust in times of crisis: Storytelling and change communication in an airline company. *Corporate Communications: An International Journal*.

Li, Y., Rho, E. H. R., & Kobsa, A. (2022). Cultural differences in the effects of contextual factors and privacy concerns on users' privacy decision on social networking sites. *Behaviour & Information Technology*, *41*(3), 655-677.

Liao, S., Wilson, C., Cheng, L., Hu, H., & Deng, H. (2020, December). Measuring the effectiveness of privacy policies for voice assistant applications. In *Annual Computer Security Applications Conference* (pp. 856-869).

Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys (CSUR)*, 54(2), 1-36.

Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43-109.

Lythreatis, S., Singh, S. K., & El-Kassar, A. N. (2022). The digital divide: A review and future research agenda. *Technological Forecasting and Social Change*, 175, 121359.

McLeod, C. (2021). Trust. In E.N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. https://plato.stanford.edu/archives/fall2021/entries/trust/

McMyler, B. (2011). *Testimony, Trust, and Authority*, Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780199794331.001.0001

Nolin, J. M. (2020). Data as oil, infrastructure or asset? Three metaphors of data as economic value. *Journal of Information, Communication and Ethics in Society*, *18*(1), 28-43.

Orlikowski. W. (2007). Sociomaterial Practices: Exploring Technology at Work. Organ. Stud.28, 9, 1435-1448.

Passi, S., & Jackson, S. J. (2018). Trust in data science: Collaboration, translation, and accountability in corporate data science projects. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), 1-28.

Prasanna, R. P. I. R., Jayasundara, J. M. S. B., Naradda Gamage, S. K., Ekanayake, E. M. S., Rajapakshe, P. S. K., & Abeyrathne, G. A. K. N. J. (2019). Sustainability of SMEs in the competition: A systemic review on technological challenges and SME performance. *Journal of Open Innovation: Technology, Market, and Complexity*, 5(4), 100.

Raj, A., Dwivedi, G., Sharma, A., de Sousa Jabbour, A. B. L., & Rajak, S. (2020). Barriers to the adoption of industry 4.0 technologies in the manufacturing sector: An inter-country comparative perspective. *International Journal of Production Economics*, *224*, 107546.

Robbins, B. G. (2016). What is trust? A multidisciplinary review, critique, and synthesis. *Sociology compass*, 10(10), 972-986.

Rousi, R. (2014). Unremarkable experiences-Designing the user experience of elevators. *Swedish Design Research Journal*, 11, 47-54.

Saariluoma, P., Karvonen, H., & Rousi, R. (2019). Techno-trust and rational trust in technology–A conceptual investigation. In *Human Work Interaction Design. Designing Engaging Automation: 5th IFIP WG 13.6 Working Conference, HWID 2018, Espoo, Finland, August 20-21, 2018, Revised Selected Papers 5* (pp. 283-293). Springer Cham.

Saariluoma, P., & Rousi, R. (2015). Symbolic interactions: towards a cognitive scientific theory of meaning in human technology interaction. *Journal of Advances in Humanities*, 3(3).

Santos, C., Rossi, A., Sanchez Chamorro, L., Bongard-Blanchy, K., & Abu-Salma, R. (2021, November). Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society* (pp. 187-194).

Saunders, M. N. (2012). Organizational trust: A cultural perspective. *Development and Learning in Organizations: An International Journal*, 26(2).

Steven S. (1994). A Social History of Truth: Civility and Science in Seventeenth Century England. Chicago: University of Chicago Press

Steven S., & Schaffer, S. (1985). Leviathan and the Air-Pump: Hobbes, Boyle and the Experimental Life. Princeton: Princeton University Press.

Tandon, A., Dhir, A., Almugren, I., AlNemer, G. N., & Mäntymäki, M. (2021). Fear of missing out (FoMO) among social media users: a systematic literature review, synthesis and framework for future research. *Internet Research*. doi:10.1108/INTR-11-2019-0455

Toulouse, E., Lafont, B., Granier, S., Mcgurk, G., & Bazin, J. E. (2020). French legal approach to patient consent in clinical research. *Anaesthesia Critical Care & Pain Medicine*, 39(6), 883-885.

Van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. *Journal of consumer policy*, 42, 91-107.

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, 42, 425-440.