Wall, Marco

Article

One User – Two Viewpoints? An Examination of Information Privacy Concerns from the Employee and Consumer Perspective

Junior Management Science (JUMS)

Provided in Cooperation with:
Junior Management Science e. V.

Suggested Citation: Wall, Marco (2022) : One User – Two Viewpoints? An Examination of Information Privacy Concerns from the Employee and Consumer Perspective, Junior Management Science (JUMS), ISSN 2942-1861, Junior Management Science e. V., Planegg, Vol. 7, Iss. 4, pp. 986-1000, https://doi.org/10.5282/jums/v7i4pp986-1000

This Version is available at:
https://hdl.handle.net/10419/295009

Junior Management Science 7(4) (2022) 986-1000

Junior Management Science

journal homepage: www.jums.academy

One User – Two Viewpoints? An Examination of Information Privacy Concerns from the Employee and Consumer Perspective

Marco Wall

Ludwig-Maximilians-Universität München

Abstract

This study aims to answer two questions about the investigation of privacy concerns in the use of video call applications: Firstly, it aims to find out how privacy concerns of users of these technologies differ in the work context from the private context. Secondly, this paper wants to discover the underlying cause for these differing concerns. To answer these questions, focus group interviews were conducted with users who use video call applications in both the business and personal contexts. The results of the qualitative research were presented visually using a thematic map. Users expressed great privacy concerns regarding the control of sensitive data. In addition, work behaviour and employment relationships are becoming more transparent, which raises more concerns. Employees in particular try to protect private, confidential data at work. This paper presents one of the first exploratory findings in the field of privacy research in the workplace.

Keywords: Information privacy; privacy concerns; online privacy; video call applications; workplace privacy.

1. Motivation

The rapid speed of technological development and competition among technology providers has facilitated the adoption of information technology (IT) by individuals and organizations (Moshki & Barki, 2014, p. 2). This digital transformation is leading to a growing number of user data being automatically generated, collected, and evaluated. Due to the increasing transparency of data, the issue of privacy is becoming increasingly important. Recent public opinion polls revealed that "*72 percent*" of the consumers "*are concerned that their online behaviors were being tracked and profiled by companies*" (Consumers-Union, 2008; Smith, Dinev, & Xu, 2011, p. 990). Most of the personal information is being used (by large companies like Google, Microsoft etc.) for tailored advertising, which is also shared with hundreds of affiliated companies. In addition, there is a risk of personal data being lost or stolen, which makes the issue of privacy even more important (e.g. Gomez, Pinnick, & Soltani, 2009, p. 14; Smith et al., 2011, p. 990). According to the Pew Research Center, 74% of participants say it is "*very important*" to be in control of their personal data (Epic, 2020).

Since the concept of information privacy is a latent concept and therefore cannot be measured directly, Information System (IS) scholars use privacy concerns as a proxy for assessing privacy in empirical research (Smith et al., 2011, p. 997). Despite the progress made by previous IS research, the nature of IT-related privacy concerns varies between several studies. Some studies emphasize context-specific privacy concerns (e.g. Jiang, Heng, & Choi, 2013; Xu, Dinev, Smith, & Hart, 2011; Xu, Teo, Tan, & Agarwal, 2012), while other researchers highlight general constructs of privacy concerns related to IT (Hong & Thong, 2013). Previous research has examined privacy concerns related to IT mainly focusing the consumer perspective, only little is known about privacy concerns in the workplace (e.g. Becker, 2018; Connolly & McParland, 2012; Moshki & Barki, 2014). The issue of privacy concerns from an employee perspective has been particularly raised by home office and remote work regulations. Following the outbreak of the Covid-19 pandemic (and government regulations to ensure social distancing) video call applications like Zoom, Skype, Microsoft Teams etc. have become popular solutions to replace face-to-face meetings with virtual meetings (e.g. Kagan, Alpert, & Fire, 2020; Wiederhold, 2020). Nevertheless, there are already some articles which criticize especially the video call application "Zoom" mostly because of its lack of security standards. Specific privacy policies of the application allowed Zoom to gain access to personal data of the users (e.g. Murphy 2020; Wagenseil 2020). In addition, hackers were able to gain access to webcam content and engage in video conference meetings

DOI: https://doi.org/10.5282/jums/v7i4pp986-1000

(Chawla, 2020, p. 2). This current practical example thus also demonstrates the increasing importance of privacy.

This bachelor thesis is therefore going to draw a comparison between privacy concerns of consumers and employees with the use of digital technologies (especially for communication). Due to the lack of literature regarding workplace privacy, the paper will focus more on the concerns in the working environment.

Hence, this paper aims to address the following research questions:

- *RQ1: What are employee privacy concerns and how do they differ from consumer privacy concerns?*
- *RQ2: Why do privacy concerns between both perspectives differ?*

The objective is to obtain relevant findings for research and business in this area, which make the current situation easier to understand and therefore also important for the future of such technologies.

Firstly, important terms such as privacy and privacy concerns are explained, especially in the context of digital technologies, and the current state of research is examined. To gain a deeper understanding of privacy concerns, especially for digital communication applications, semi-structured focus group interviews with experts of these applications were conducted. Afterwards, the results of this evaluation will be discussed. Important limitations and implications will be shown.

Finally, the paper concludes with a presentation of the overall results in compact form and gives a brief outlook on future developments.

2. Theoretical Background

2.1. Terminology / Important Terms

The concept of Informational Privacy is an area of research that is being explored in a variety of research fields, including law, economics, psychology and many others (Bélanger & Crossler, 2011, p. 1018; Pavlou, 2011; Smith, Dinev, & Xu, 2011). This paper aims at exploring the construct of information privacy within the information system domain. The worldwide use of the Internet is increasing continuously. Users' personal data is often collected, stored and analyzed. Therefore, privacy concerns in particular are becoming increasingly important in the digital age (Smith et al., 2011, p. 990). Advances in information and communication technology are opening new forms of exchange, thus also making the issue of privacy more important (Archibald, Ambagtsheer, Casey, & Lawless, 2019, p. 1). The introduction of so-called video call applications (often known as Voice over Internet Protocol (VoIP)-mediated technologies, in the context of this work hereafter limited to the first term) "*allow for real-time interaction involving sound, video, and often, written text*" (Archibald et al., 2019, p. 2; Weiler, Matt, & Hess, 2019). Such technologies therefore replicate features of face-to-face meetings and offer unique advantages, but also challenges, particularly in terms of privacy (Lacono & Brown, 2016, p. 1-3). For better understanding, the most important terms from the field of information privacy research are explained in the following section.

2.1.1. Definition Information Privacy

Privacy covers many areas of human life, is used in many disciplines and is therefore a collective expression (Buck & Dinev, 2020, p. 4232; Solove, 2005), which needs to be defined more precisely and clarified for the context of the use of information systems (Buck, 2018, p. 13). In the literature, privacy is not uniformly defined and is often not precisely delimited with regard to the respective object of investigation (Smith et al., 2011; Solove, 2005). Smith et al. (2011) classify the concept of privacy into the areas of physical privacy and information privacy. While physical privacy addresses the individual and/or the individual's surroundings and private space, information privacy addresses the action and responsibility dimension of the personal information (Smith et al., 2011, p. 990). Furthermore, the term is described as a multidimensional, elastic, and dynamic construct, which must be separated from overlapping concepts like confidentiality, secrecy, anonymity, security, and ethics (Smith et al., 2011, p. 995). Clarke (1999) identifies four dimensions of privacy: "*privacy of a person, personal behavior privacy, personal communication privacy, and personal data privacy*" (Connolly & McParland, 2012, p. 32). Due to the digitalization of information and communication, Bélanger and Crossler (2011) argue that the dimensions "personal communication privacy" and "data privacy" can be merged into the construct of information privacy (Pavlou, 2011, p. 978).

Because of the object of investigation of information systems for communication, this paper focuses on the dimension of information privacy. The definition of information privacy is directly linked to the development of information systems and therefore has different perspectives of definition (e.g. Dinev & Hart, 2006; Krasnova & Kift, 2012; Nissenbaum, 2009). A fundamental discussion is held with the perspective of privacy as a moral or legal right (Warren & Brandeis, 1890). With the perspective on privacy as a state, Westin (1968) and Altman (1975) introduce a way of looking at the individual and situational context of the user. The relationship to other individuals and privacy as a "*state of limited access to information*" (Smith et al., 2011, p. 995) becomes important. Moreover, the control-defined definition of privacy as a scientific discourse is becoming increasingly relevant (Altman, 1975; Smith, Milberg, & Burke, 1996; Westin, 1968). Margulis (1977) describes privacy as *"the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability."* (Margulis, 1977, p. 10).

The concept of self-determined and autonomous control over the disclosure of personal information is closely related to the development of information technology and information systems (Buck, 2015, p. 107; Dinev & Hart, 2006). As

information systems evolve and expand, the collection, processing, and storage of personal information increases.

Especially when using information systems for communication, users release their personal data for the purpose of obtaining digital services. Individuals have the right to protect themselves from unwanted access in the sense of an intrusion into personal data (Rössler, 2001). This often leads to concerns when using such technologies. These will be examined below in more detail.

2.1.2. Definition Information Privacy Concerns

With increasing digitization and rising use of digital information systems, user concerns regarding information privacy are growing. Since the concept of information privacy is a latent concept and therefore cannot be measured directly, almost all empirical privacy research relies on the concept of information privacy concerns as a proxy for privacy (Smith et al., 2011, p. 997). Due to the broad scope of these concerns, different perspectives and definitions of privacy concerns have been developing in the scientific discourse.

Privacy concerns can be defined as user concerns about a possible future loss of privacy as a result of voluntary or involuntary disclosure of personal data (Dinev & Hart, 2006, p. 65; Reith, Buck, Walther, Lis, & Eymann, 2019, p. 3). This definitional approach is also shared by Malhotra, Kim, and Agarwal (2004) who defines privacy concerns as an individual's subjective view of fairness within the context of information privacy. A more restrictive definition of privacy concerns is used by many researchers, defining them as concerns that users have about the way companies and organizations handle personal data (Buck & Dinev, 2020, p. 4232; Smith et al., 1996, p. 169).

Privacy concerns hence strongly influence the behavioral intentions and the actual behavior of individuals when revealing private information (Pavlou, 2011, p. 982). Therefore, the goal of scientific studies is primarily to analyze the consequences and effects of privacy concerns. In this context, the construct of privacy concerns serves as an antecedent for several behavioral variables, e.g. willingness to disclose personal information (Chellappa & Sin, 2005), intentions to transact (Dinev & Hart, 2006) and information disclosure behavior (Buchanan, Paine, Joinson, & Reips, 2007; Xu et al., 2011, p. 800). IS studies see the construct of privacy concerns mostly as a general construct reflecting the inherent concern of individuals about the possible loss of privacy (e.g. Malhotra et al., 2004; Smith et al., 2011). However, recent legal and social scholars have noted that privacy is maybe more situation-specific than dispositional, making it important to distinguish between general concern and situation-specific concerns (e.g. Margulis, 2003; Solove & Hoofnagle, 2006; Xu et al., 2011, p. 800).

Today's privacy studies investigate the topic of privacy concerns in various contexts, e.g. in e-commerce or in social media. However, empirical research on privacy predominantly uses three constructs for privacy concerns as the base construct. These will be examined in the following chapter "Current State of Research".

2.2. Current State of Research

Previous research investigating the effects of privacy concerns has mainly focused on the intentions of using various types of online services (Bélanger, Hiller, & Smith, 2002, p. 247), disclose of personal information, engagement in e-commerce transactions (Dinev & Hart, 2006), and undertaking online purchases (Pavlou, 2011, p. 979). A major focus of the research lies on the individual level, especially on the consumer side. Bélanger and Crossler (2011) propose that more studies need to be conducted at the group, organizational, and societal level by viewing information privacy as a multilevel concept (Pavlou, 2011, p. 979). Hereby, there are still very few studies on the subject of privacy in the workplace, especially with regard to privacy concerns related to the use of IT (PCIT) (Becker, 2018; Connolly & McParland, 2012; Moshki & Barki, 2014). The following section will focus more on the privacy concern constructs on the consumer side and research concerning privacy in the workplace. In chapter 2.2.3 this paper tries to combine both strands of research and show why it is necessary to empirically investigate privacy concerns, especially in the employee sector.

2.2.1. Privacy in the Consumer Perspective

In empirical privacy research, three main constructs are used for privacy concerns. The Concern for Information Privacy (CFIP) is the first developed and validated construct used to measure information privacy concerns (Smith et al., 1996; Stewart & Segars, 2002). Malhotra et al. (2004) later developed a measuring instrument called the Internet Users' Information Privacy Concerns (IUIPC), which tries to be more specific to the technological conditions of the Internet. With the Mobile Users' Information Privacy Concerns (MUIPC) a construct was developed, which focuses on the privacy concerns which takes into account the environment as well as the specificities of privacy concerns in the context of mobile systems (Buck, 2018, p. 20; Xu et al., 2012). However, all three constructs contain large overlaps in terms of measuring instruments and dimensions. Due to the constant development of different information technologies, however, the number of different situation-specific constructs increases.

Today, one of the most important information privacy concerns in IS research is the construct of Internet Privacy Concerns (IPC). The Internet is one of the most popular mediums through which consumer and organizational data is transmitted, collected and analyzed (Hong & Thong, 2013, p. 276). IPC reflect an individual's perception of user concerns for how personal information is handled by websites. This can be different from users' expectations of how websites should handle users' personal information. Caused by the growing digitalization and the related implementation of digital technologies and new information system, the number of different conceptualizations of the IPC also increased (Hong & Thong, 2013, p. 278). Nevertheless, there are six key dimensions that are most commonly utilized of IPC. They are Collection, Secondary Usage, Errors, Improper Access, Control, and Awareness. Although the field of privacy concerns in the use of video call applications has not yet

been investigated, an attempt is being made to identify these dimensions. The dimensions have the following meanings:

Unauthorized Secondary Use addresses users' concerns that "*personal information is collected for one purpose but is used for another, secondary purpose without authorization from the individual*" (Hong & Thong, 2013, p. 278; Smith et al., 1996, p. 172). The construct *Error* addresses users' concerns about data inaccuracies. It is the degree to "*which a person is concerned that protections against deliberate and accidental errors in personal data collected are inadequate*" (Hong & Thong, 2013, p. 278; Smith et al., 1996, p. 172). *Improper access* describes "*privacy concerns with respect to the perceived threat of unauthorized access by third parties*" (Becker, 2018, p. 3262; Smith et al., 1996, p. 172). The dimension *Collection* describes the "*subjective concern with respect to the accumulation of personal information*" (Becker, 2018, p. 3262; Smith et al., 1996, p. 171). *Control* is the degree to which "*a person is concerned that users do not have adequate control over their personal information*" (Hong & Thong, 2013, p. 278; Malhotra et al., 2004, p. 339). Lastly, *Awareness* is the degree to which a "*person is concerned about users awareness of information privacy practices*" (Hong & Thong, 2013, p. 278; Malhotra et al., 2004, p. 339). The level of analysis of the IPC construct is mainly used with consumer data.

2.2.2. Privacy in the Employee Perspective

Privacy at the workplace is a field of research that has not yet been investigated as extensively as the field of consumer perspective. Due to the questions how privacy is defined in the workplace, scholars have identified three specific organizational contexts where employee privacy matters: First, regarding their information (information privacy), their workplace (work environment privacy) and their ability to work autonomously (autonomy privacy) (Bhave, Teo, & Dalal, 2020, p. 131; Stone & Stone, 1990). Although there is an overlap of the three concepts, the present work focuses on the concept of information privacy. Information privacy in the workplace includes the type of information on employees collected by organizations, the source of the information collection, the purpose of the information collection, and how the information is stored and used (e.g Bhave et al., 2020, p. 137; Smith et al., 1996; Stone & Stone, 1990).

Furthermore, the question arises for which different stakeholders privacy matters. The key stakeholders in workplace privacy research are employees, employers, and the state (Bhave et al., 2020, p. 132). The interests of the individual parties differ here: Employees strive for income and fulfilment; employers desire profit maximization and ensuring stakeholder value; the state wants to safeguard freedom and ensure the rule of law (Budd & Bhave, 2008). However, a strong focus lies on the employment relationship, which is the "*connection between employees and employers through which individuals sell their labor*" (Budd & Bhave, 2010, p. 51). Both stakeholders possess a privacy calculus where they engage in a cost benefit analysis where they weight risks of disclosing information versus withholding (Culnan & Armstrong, 1999; Laufer & Wolfe, 1977). For the employees' privacy calculus, the main risk associated with providing (or accessing) information is the perception of invasion of privacy in connection with the potential loss of control over one's own information (Bhave et al., 2020, p. 133; Stone & Stone, 1990). On the other hand, the key benefit in providing information is the reduction of information asymmetries that exist between them and the employer. Organizational risks when collecting employees' information are a potential invasion of the employees' privacy, the associated detrimental effects as well as the negative impact on employee morale and/or the organization's brand (Bhave et al., 2020, p. 133; Culnan, Smith, & Bies, 1994). The main benefit for the organization when possessing superior information about its employees is making better employment-related decisions and thereby increasing the security of the organization and reducing its legal liability. Both calculus models influence each other and can also be influenced by macro factors (Bhave et al., 2020, p. 134).

In the following section this paper will investigate the employee side and the reasons for possible concerns about their privacy. The issue of privacy concerns from an employee perspective has been particularly raised by home office and remote work regulations. Due to the increased use of digital technologies and new information systems (especially for internal communication), the topic of privacy is becoming more and more important.

2.2.3. Literature Review: Differences in Both Perspectives

There are only very few studies on information privacy research that have been carried out at all levels except the individual level. Investigative literature in the area of privacy concerns about communication technologies is very limited (Smith et al., 2011, p. 1004). Literature in organizational analysis based on communication technologies is outdated. Most of the work is conducted on the individual level, because there are validated concepts that can be used for the research and it is easier to collect and analyze data from a large number of people through surveys or interviews (Bélanger & Crossler, 2011, p 1028). However, despite the high level of research in the field of Information Privacy Concerns, there is only a small effort in developing tools for individuals to protect their information privacy. In addition Bélanger and Crossler (2011) state that most of the studies conducted at the organizational level focuses on information privacy practices as well as instituting appropriate policies. One possible explanation for the lack of organizational research shows that while organizations are interested in understanding the implications of information privacy impacts, researchers have not yet addressed these issues. Collecting information from citizens or consumers in general is easier than encouraging organizations to participate in such surveys.

However, the implementation of new information technologies is also becoming increasingly important in the workplace. Data on employees can be easily analyzed and evaluated, thus increasing the issue of surveillance (Connolly & McParland, 2012). Even if user data is not necessarily col-

lected specifically for monitoring employees, privacy concerns are increasing when using digital technologies. Privacy concerns have the potential to negatively affect organizational productivity and employee morale (Connolly & McParland, 2012, p. 32).

To further advance research in the organizational field, this paper tries to find more insights into the information privacy concerns of employees and to compare them with consumers. The next chapter deals with the chosen methodology for answering the two research questions.

3. Methodology

Since previous research has only examined privacy concerns on the consumer side, a qualitative approach is chosen to explore privacy concerns in the emerging workplace context (Myers, 2009). Interviews will be conducted to ask employees about their privacy concerns and examining how they differ from consumer privacy concerns. Due to the lack of research in the workplace context, the coding of the employee privacy concern is inductive based on the Grounded Theory by Glaser, Strauss, and Strutzel (1968). Consumer privacy concerns are coded inductively and deductively because certain codes are matched with dimensions of existing literature. All codes, factors and dimensions are finally combined inductively and deductively with the iterative thematic analysis approach (Braun & Clarke, 2006, p. 83).

3.1. Choice of Interview Partners

Concerning the choice of interview partners, this paper covers a heterogeneous sample of participants (Patton, 1990, p.169) that use digital video call applications (like Zoom; Skype etc.) in a private as well as in a workplace setting in order to cover their perspectives as a consumer and as an employee. As focus groups are especially well suited to uncover and document the “why” behind opinions, and in obtaining more depth and breadth in the analysis of participants, this paper conducts semi-structured focus group interviews (e.g. Becker, 2018, p. 3263; Morgan, 1996, p. 130-131). In focus group interviews participants have the opportunity to query each other, explain themselves and comment on each other’s experiences (Kitzinger, 1995, p. 299). This research method has been already used to uncover privacy aspects, like privacy concerns about technologies and acceptance of new technologies (Morton, 2014, p. 270). In the selection of interview partners this paper will follows the recommendations of Marshall, Cardon, Poddar, and Fontenot (2013) to collect data until data saturation is achieved.

Due to the psychological complexity of privacy concerns, this paper uses an iterative thematic analysis approach to structure the heterogeneous privacy perceptions into homogeneous themes to compare and analyze the influencing factors on privacy concerns of video call application users (Becker, 2018, p. 3261).

3.2. Data Collection

Three focus groups – are considered to be an adequate number (Morgan, 1996)- with 5-6 participants per group took place, capturing the views of 18 individuals. To ensure participants represent a broad range of experiences and ages, this paper uses opportunistic sampling with peer sampling for all three focus groups. 10 of the interview partners were female, 8 were male. The average age was 38 years. The age of the users ranged from 20 years to 63 years. An overview containing demographic profiles of the participants can be found in Table 1. All participants use video call applications to communicate with various stakeholders.

The group is designed to encourage the participants to interact with each other rather than with the researcher, to allow "*structured eavesdropping*" (Kitzinger, 1995, p. 301). At the beginning of each focus group the researcher provided an overview of the objectives of the study. In addition important terms like privacy and privacy concerns were explained. After questioning demographic data, the usage behavior of video call applications was examined. Next, the researcher attempted to restrict the contribution to reading the following open-end questions out loud, and asking further when required:

1. Do you have privacy concerns when using digital technologies at work?
2. In contrast, what are your privacy concerns in a private setting?
3. How do your privacy concerns differ (when using digital communication technologies) between private use and work use?
4. Why do your privacy concerns differ?

Each focus group lasted approximately from 45 minutes to one hour, 10 minutes asking participants about their demographic data and their usage behavior with the examined technology. Afterwards about 20-30 minutes were spent on questioning the privacy concerns on the employees’ side. It followed with an analysis of how these concerns differed from their private ones. An important subject of the investigation was also the reasons for the differences.

The same questions and procedures were used for each focus group facilitating an investigation into the similarity of the themes discussed across the focus groups (Morton, 2014, p. 272).

3.3. Data Analysis

The interview evaluation is based on the iterative thematic analysis approach to find patterns within the data (Braun & Clarke, 2006, p. 83). This analysis is particularly suitable for sensitive data environments (Patton, 1990) and is frequently employed in IS research (e.g. Becker, 2018, p. 3263; Weiler et al., 2019, p. 5881).

Each focus group interview was held via the video call application Zoom. The use of Zoom as a qualitative data collection tool has already been reviewed in the literature (Archibald et al., 2019). Solely the audio material was

Table 1: Demographic Profile of Participants

Demographics		**Number of Respondents**
Gender	Male	8
	Female	10
Age *(Average)*	Focus Group 20-30	21,8
	Focus Group 30-40	34,4
	Focus Group 40+	54,4
Working Situation *(Average)*	Home Office	65%
	Office	35%
Videocall Applications *(Business Setting)*	Zoom	12
	Microsoft Teams	16
	Cisco WebEx	2
	Skype for Business	2
	Apple FaceTime	1
	KUDO Meetings	1
Industry Sector / Department	Banking Industry	2
	M&A	1
	Consulting	2
	Big Media & Entertainment Company	1
	Luxury Goods:	
	- Off-Trade	2
	- Human Resources	3
	- Logistics	1
	- Marketing	1
	-On-Trade	1
	- Travel Retail	1
	- Management Assistant	1
	- IT	1
	- Customer Service	1

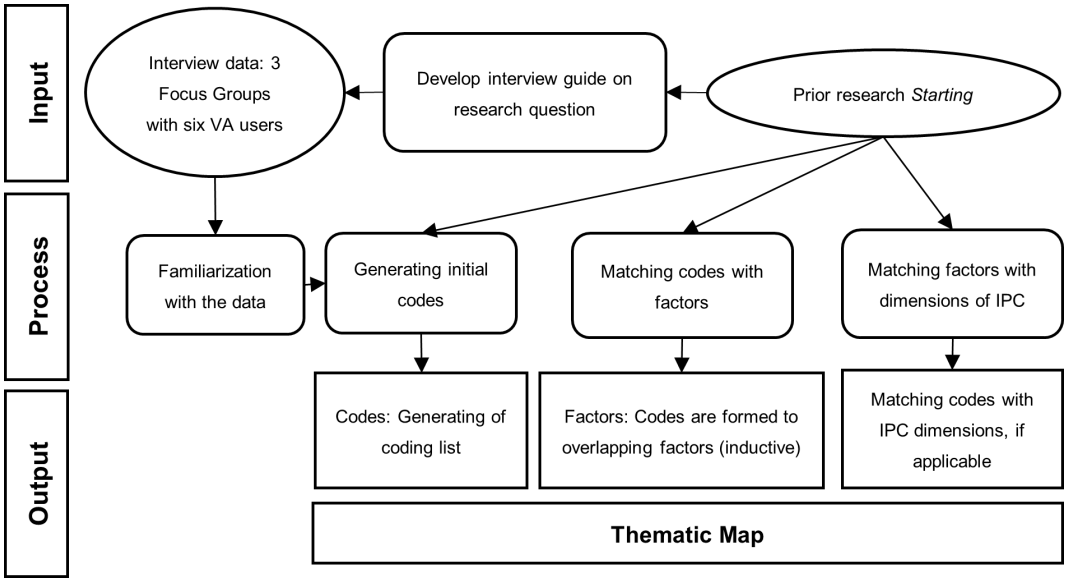

Figure 1: Iterative Thematic Analysis Approach based on Becker (2018)

recorded and first transcribed using "AmberScript", an AI-based software tool that converts audio material into text. The transcript was then repeatedly proofread. Later, the transcripts were uploaded to ATLAS.ti, one of the most widely used software for qualitative data analysis by IS researchers, to generate initial codes by searching for recurring patterns in the raw data (e.g Becker, 2018, p. 3263; Morton, 2014, p. 272). The entire transcript from each focus group was coded to ensure "*each data item has been given equal attention in the coding process*" (Braun & Clarke, 2006, p. 96). The concerns as a consumer are coded both inductively and deductively in order to include existing literature. The generation of employee concerns is inductive. The conceptual basis of the coding process hereby was drawn from already validated privacy concern constructs (e.g. IPC construct (Hong & Thong, 2013), which describes consumer privacy concerns in an online setting).

This paper identifies 56 different codes in the data set. In the next step different codes like "permanent accessibility" were merged with factors like "Performance tracking". Factors were then combined into different dimensions. The process of matching codes with the factors, and then the factors with potential dimensions of already validated privacy concern constructs (e.g. IPC) was accompanied by a constant review of the literature.

4. Results

4.1. Differences in Employee Privacy Concerns to Consumer Privacy Concerns

The first question to be answered is how privacy concerns differ in the use of video call applications as an employee to the use of these applications in private settings. The thematic map (Figure 2) visualizes the results and includes both dimensions derived from the theoretical part of the existing literature on privacy concerns and new dimensions from data collection of the interviews. It is composed of 7 dimensions Control, Collection, Awareness, Errors, Employment, Improper Access, Employment Status, and their related 13 factors. Factors and dimensions will be described in the following section.

4.1.1. Control

The Control dimension covers an individual's concerns that they do not have adequate control over their personal/firm information when using video call applications (cf. Becker, 2018, p. 3266; Malhotra et al., 2004, p. 339). Two factors were analyzed inductively to this dimension.

Dilemma of Usage by Confidential Data: Users express concerns about data control when highly confidential information is involved in communication. It is evident that consumers are switching to alternative technologies to gain more control over data, both in the workplace and in their private lives. In the working context two different types of disuse of video call applications can be distinguished. Firstly, the employer prohibits sharing of certain data on the video call applications. Participants stated that passwords and personal data of employees (especially mentioned in the human resources department) are never shared via the platforms: "*most of the data will be sent by email and not per the data sending tools on Teams"* [P2G1]. Another participant noted: "*the type of documents we have (i.e. human resource department) often prohibits sending them via Zoom*" [P4G2] In this regard, one user stated that there are specific guidelines in which data can be shared with the respective technology*: "I had eLearning in which I have learned what kind of data I am allowed to deliver via which platform. So, a few things I am only allowed to send via email and only encrypted and a few things only via shared folders. In general, I am not allowed to send data via Microsoft Teams or similar application. So, it always has to be encrypted and safe"* [P4G1].

Secondly, users are switching to other technologies they feel more comfortable using and where communication can be better controlled: *"I am super unwilling to send sensitive data over MS Teams, such as an internal price calculation, because it is easier to make mistakes or address someone else incorrectly. I still tend to do important things simply by email, [. . .] because of their clear traceability. Besides, I do not trust the whole thing 100 per cent that it is safe there. Especially with such sensitive data such as customers, prices etc."* [P2G2]. The missing or complicated "*trackability*" [P4G2] of communication in video call applications leads to the use of other technologies such as email.

Also, in the private sphere, participants tend to communicate sensitive messages by phone or in person: *"do not share your passwords or private sensitive data on any of those conversations [. . .]. And I think most of us do not like typing the password via WhatsApp. I called him and told him by phone"* [P3G1]. The use of the telephone as the main communication tool was often mentioned in this context: "*When it really comes to very personal things and serious topics, I prefer to use the telephone"* [P4G3].

Spread of Digital Content: This factor describes the concerns of employees and consumers about the uncontrolled loss or distribution of data using video call applications. Especially when traveling, video call applications are rarely used in the working context to avoid the risk of eavesdropping: *"I would have some concerns with that (i.e. travelling) because I could not guarantee that if I am speaking to someone on the phone or having a call with someone that I am actually taking the measures that their data does not go to someone sitting next to me"* [P3G1]. Another aspect that has been raised in this context is the one-sided control with communication tools like video call application*: "you can only control your outgoing side and you can only take as many precautions as you want, but it's only from your side."* [P3G1]. Concerns about uncontrolled distribution have also been expressed in the private sector: "*WhatsApp is actually more of a communication tool where things get relatively outspoken from time to time [...] there are simply chats where you can't control what the others contribute*" [P8G3]. The last concern that has been made in this context refers to the increased number of different communication technologies that are implemented

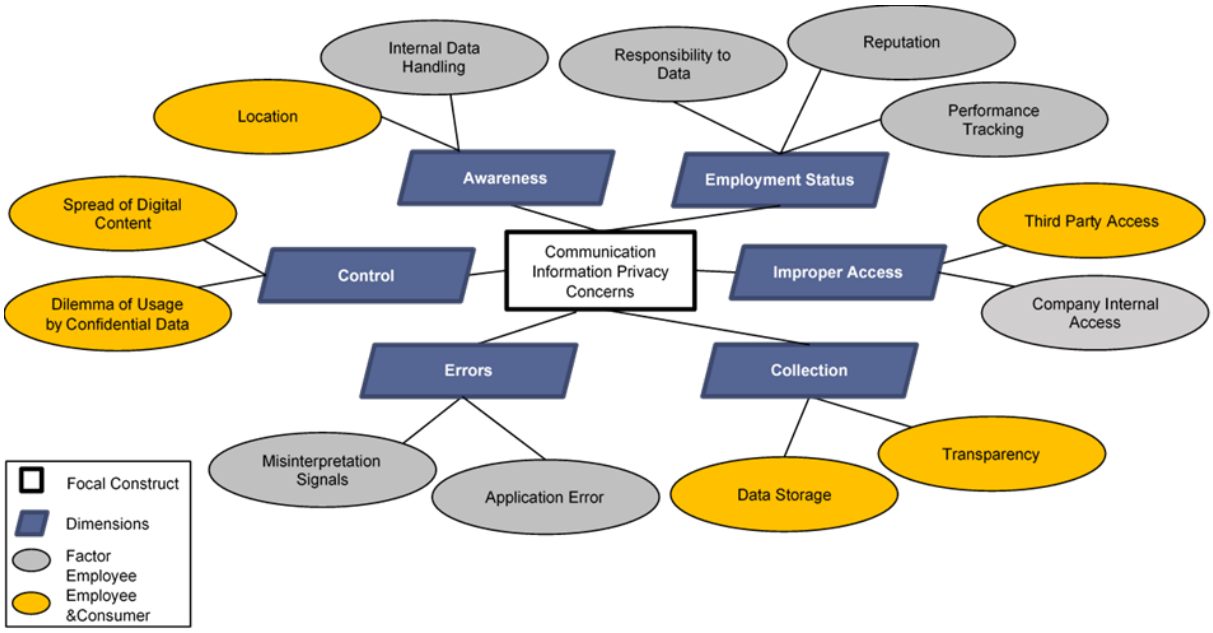

Figure 2: Thematic Map of Privacy Concerns of Employees and Consumers of Communication Technologies

in companies, which tends to lead to a weakening of communication: *"There are simply far too many communication strains and they are being opened up nowadays. And that is a problem, as at some point information gets lost, since you lose the overview, because everyone loses overview"* [P6G2]. Multiple informal forms of communicating and risk of uncontrolled data transfer were described as a "*Chinese-whispers-phenomenon (German Stille-Post-Phänomen)* "[P6G2] among the participants.

4.1.2. Improper Access

The dimension of Improper Access covers individuals' concerns that video call applications do not have adequate measures in place to prevent unauthorized individuals or organizations from accessing personal/firm information or that through the use of such technologies, data may be disclosed to third parties. (cf. Becker, 2018, p. 3265; Smith et al., 1996, p. 173). By analyzing the data, two factors could be found for Improper Access.

Third Party Access: Describes the unauthorized access to personal and firm data by third parties actively or passively while using the applications. This factor was mainly mentioned in the private context, as it is assumed that organizations provide the necessary safety precautions in the workplace: *"If there are difficulties or problem in the security, it is the responsibility of the company to solve them"* [P4G3]. The main concern is that third parties actively eavesdrop or monitor confidential communications, therefore one user mentioned: *"you cannot be sure if there will be a tape at the end (i.e. persons recording meetings). You are never really clear about that, who can see and who cannot."* [P4G2]. Concerns arise in the private sphere when internal family information would be disclosed: *"If my dad tells me some information about his business, it is a private and familiar topic which other people should not know"* [P5G1].

Company Internal Access: This factor describes the concern that personal data could be disclosed within the company to employees or supervisors who should not have access to it. Especially the exchange of private information in a business environment is a sensitive issue, as "*the borders*" between private and professional sphere are often "*floating*" [P8G3].

Users express concerns that private sideline activities made during business meetings may be noticed and picked up by other employees: *„When I get a phone call during a meeting, I am concerned that the conversation will be audible to the other 300 people in the meeting"* [P5G2]. Another user expressed the concern "*that someone is walking through the background or that you have an unfavorable setting with regard to the camera*" [P6G2]. Virtual backgrounds are often used as a security precaution in this context. In addition, the risk of private information being shared between individual employees to other employees/ or the entire team was a common concern: *"Writing stuff about, 'hey, maybe you can make that better or something that like this', what is private information about the team member. And it is not for all the members"* [P5G1].

On the other hand, there is a concern that outside of the work environment, communication about work or other employees may have negative effects when it leads back to the organization: *"when we will have a call or talk privately about work stuff or stuff that happened at work and it would not be great if stuff like that goes out. So, there are concerns"* [P7G1].

4.1.3. Employment Status

The Employment Status dimension includes individuals' concerns that the use of video call applications may have a negative impact on the employment relationship, especially towards the supervisor as well as other employees. This dimension was only mentioned in the context of workplace privacy concerns. Moreover, this dimension was analyzed inductively from the data.

Performance Tracking: This factor describes the increased transparency and traceability by the application, which becomes an increased challenge. Status notifications in applications such as Microsoft Teams and Skype for Business are seen by users as an "*additional obligation"* and access to the individual, as the application "*requires you to be available all the time*"[P8G3]. The transparency of work behavior in particular gives rise to concerns, which are expressed as follows: *"you can see (i.e. related to Microsoft Teams) via the green or yellow or red round indicator, if I am sitting at my computer or if I am in a meeting and so on. . . "* [P4G3].

Reputation: Especially in the young focus group (i.e. 20-30 years), maintaining a good reputation at the workplace is particularly important. Before a video call meeting, security precautions are therefore taken: *"I close all tabs (i.e. other programs) because I do not want to get any one from my colleagues see that I'm doing nonworking stuff in my working time"* [P3G1]. When using the option of screen sharing, people are concerned that private information is visible, which could give a negative impression about the person*: "If I have to do some screen sharing and I have that (i.e. private messenger) open and everybody could read my messages, I would not like that. I want to leave a good impression"* [P2G1]. It is noticeable that one's visible surroundings, especially in video calls, has a strong influence on the reputation. One user felt uncomfortable conducting meetings outside his or her usual workplace: *"I noticed that I did not participate that much in this call because I was in like a restaurant or something. And I did not want the customer to recognize that I am not in a working environment"* [P6G1]. To avoid conclusions about the working environment (increased concern due to home office), users try to have a clean background or even switch off their cameras during meetings.:" *I would avoid sitting in front of by bed, that everyone could see that*" [P4G2]. Other users do not want to provide any information about their environment. *"I do many zoom meetings or other meetings without a camera. I do not want that everyone can see my private background"* [P7G3].

Responsibility to Data: The use of company data in particular leads to increased responsibility, which also gives rise to concerns: *"when I am in the work environment, I am also responsible for the company and the company data and safety."* [P4G1]. In the event of loss of data, this does not only concern a single person but the whole company. This concern is amplified when users use private devices (e.g. private laptop) to communicate, as it may be difficult to maintain the same security measures, while other parties require the same level of responsibility. One user stated: *"when we call an external client of us, for example, or a business partner, because there we mostly call with our private phones, with our private laptops and private data [..] and there I/we or our bank cannot assure that they have the privacy standards which are needed for the sensitive data we have*" [P3G1]. Moreover, communication on company data is shown to cause increased concern among users and therefore more attention is paid to the question *"What kind of information am I processing here?"* [P6G1].

4.1.4. Awareness

The Awareness dimension refers to the individual's concern regarding their lack of awareness of how the use of video call applications utilizes and protects the privacy of personal/firm information (cf. Becker, 2018, p. 3266; Malhotra et al., 2004, p. 339). It is noticeable that users have little knowledge about the security precautions of video call applications made by the application itself or the employer.

Location: An important factor influencing awareness of whether an application perceived as safe is the place of communication or the location of the application. People are unaware of the application when it is managed by companies that are located in countries with controversial government policies: *"There is this concern for me based on the location of the company actually, or the service where the data is stored. I am not really sure if something is safer. I guess that Zoom kind of fixed these concerns. And yeah, it was a lot about media coverage and Zooms new technology, I think based in Asia*" [P6G1].

Internal Data Handling: This factor describes employees' lack of awareness of how organizations deal with internal communication data. One user posed the question*: "Who has access to your Microsoft Team?"* [P5G2]. It is noticeable that users do not know exactly who has access to the communication within the organization. Similarly, a different user poses the question: *"What opportunities do the people or departments we know have to collect data*?" [P7G3] There is a concern that data will be transferred without awareness: *"I am concerned that data may end up where I do not want it to end up"* [P5G2].

4.1.5. Error

The Error dimension refers to an individual's concerns that the application or use of the application does not have adequate measures in place to prevent or correct errors in their personal data (cf. Becker, 2018, p. 3266; Smith et al., 1996, p. 173). This dimension was mainly mentioned in the context of workplace concerns.

Application Error: This factor indicates that users are not sure whether the application or tools of the applications are working properly, and consequently personal data becomes accessible to others. When participating in video calls, it is possible to set your microphone to "mute". The correct function is questioned by a user: *"I have concern that the mute function really works, and I prefer to leave the room during a meeting"* [P5G2]. Even secondary functions such as chatting during a video call are often avoided due to potential errors. Person 4 in Group 2 states: *"Special care must be*

taken with the chat function. I am worried that a private chat will end up in the group...that is why I always look it up three times" [P4G2]. The use of the virtual background is used to avoid giving conclusions about the working environment (see Reputation). This function shows partial errors: "*The virtual background does not work for me. It shines completely through my face and that looks really creepy*" [P3G2].

Moreover, users expressed concerns about using the application when security issues were identified through media reports: "[. . .] *for example, with Zoom, that they had not well functioning privacy [. . .] security measures and that is why I think also when deciding which infrastructure to use, we didn't decide for Zoom"* [P3G1].

Misinterpretation Signals: This factor describes that certain signals (e.g. online status) in the video call applications gives false impressions about work behavior. Especially in video call applications like Microsoft Teams, as well as Skype for Business, every employee can see the presence status of every organization member via a sign symbol. One user states that: when "*the sign is yellow and it may show my team that I'm away and not working, but I am working. And then I have a little bit concerns that they can have a wrong feeling from my working habits*" [P4G1].

4.1.6. Collection

The Collection dimension captures an individual's concern that the application itself of the employer is collecting and storing large quantities of personal data through communication (cf. Becker, 2018, p. 3264; Smith et al., 1996, p. 171). Two factors were related to this dimension.

Data Storage: This factor describes that all communication via the applications is tracked and stored through the application itself as well as through the organization. One user said: "*Everything is tracked. It is not deleted, and someone has access to it."* [P3G2]. Concerns arise that communication will be monitored „*when you make a call, it may be recorded in the background and stored in the cloud*" [P5G2]. The concern that the data collected would be used against a person was particularly pronounced in the workplace: "*if you say something at work that is completely against everything* (i.e. the firm guidelines), *this can lead to dismissal"* [P5G2]. In a private setting people think that: "*in the mass that is generated, in messages, in texts, in pictures, in videos. What role do I play there?"* [P2G2].

Transparency: This factor describes the concern that personal data becomes more transparent using video call applications. Especially in the private sphere, users assume that all communication is stored somewhere in the cloud: "*I think to myself, as soon as I look for something in my mobile phone or anything else, nothing is private anymore. And as soon as you move somehow, it all ends up somewhere"* [P5G2].

4.2. Reasons for Differences in Privacy Concerns

Having identified the different privacy concerns of users in the work context as well as in the private context, the question arises why they differ:

The general trend is that privacy concerns are more widespread in the workplace than in private life. This observation can be found in all focus groups. In the youngest focus group (20-30 years), this is most noticeable, as they describe themselves as "*pretty affirm to digital technology*" [P6G1] and mainly use video call applications (e.g. FaceTime) with friends and communicate on everyday topics: "*when I FaceTime with my friends, I do not have any privacy concerns. We talk about everything and it is not top-secret private data*" [P2G1]. One user stated that the issue of data security is much more questioned in the working context: "*when you are in a business environment, there is this general more data policy stuff going on [...] you think more about it. When I use the digital technology in a business environment, I am more in the "What kind of information am I processing here?". And when I am in the private environment, I do not think about this at all, because I am like private free time. I do not have any privacy concerns*" [P6G1]. In private, the issue of data security is less considered: "*In my private life I think about it much less than I do in my business life."* [P4G2]

A potential loss of company data or incorrect handling of data in working life is considered a greater loss, as data is considered "*more valuable*" [P6G1]. In private life, users only must be aware of their own responsibility for data, while in the workplace company and customer data is also processed. One user summarized that with: "*when I'm talking with friends, I am mainly responsible for my own stuff I say and I feel more safe to handle my own responsibility with my own information, because if something goes outside, then it is my problem and I have to deal with it"* [P4G1]. There is also a concern, especially in the second focus group (30-40 years), that communication data will be screened and used against the individual. Consequences, such as dismissal, increases concerns about privacy at work compared to privacy at home: "*Privately, there are no consequences to be feared, but in the workplace if you send or do something at work and completely against everything and here is your dismissal"* [P5G2]. In private sphere, it is anticipated that mass data in general will be more interesting than individual data: "*I hope that I am one of the 7 billion that nobody cares"* [P7G3]. Interestingly, some of the older participants (40+ years) have more concerns in the private sphere, as there will be no security from the employer: "*I sometimes have the feeling that as an individual I can do so little in private. I can pay attention. I can make my password accordingly complex. But in the end, I do not have the same opportunity to build up protection as a large company"* [P4G3].

Privacy concerns about the application are lower in working life, as employees assume that professional business applications have sufficient security standards. Especially the use of well-known communications applications, which also offer other business solutions in working life, ensure trust: "*In my opinion, I think that MS Teams will be established throughout the business world because everybody is using Microsoft Office already like Excel and Word [. . .] a lot of people trust the Microsoft products in general"* [P6G1]. In addition, people are less concerned about the application, if it is only

used in a business setting: "*I think it (i.e. Microsoft Teams) feels automatically safer for companies because it's already targeting companies and therefore, yeah, it's already of their concerns*" [P7G1].

5. Discussion of Key Findings

This paper conducted a study to identify how information privacy concerns in communication with video call applications differ in a private setting to the workplace. Secondly, this paper analyzed why privacy concerns differ in the various settings. Therefore, three focus groups were interviewed about their concerns and then evaluated in a rigorous iterative thematic analysis (Braun & Clarke, 2006, p. 83). This procedure was used to create interview codes, which were combined into factors and dimensions. The data were visualized in a Thematic Map. The 4 dimensions (Awareness, Error, Collection, Improper Access) were deductively derived from existing literature (Malhotra et al., 2004; Smith et al., 1996). Factors as well as the dimension "Employment Status" were inductively generated from the qualitative data (Glaser et al., 1968). Certain statements could also be assigned to more than one concern based on their message. When analyzing the data, it becomes apparent that the three focus groups, which were classified according to age, have large differences in terms of privacy concerns. Depending on the group, different factors were mentioned in the length and frequency of the discussion, which are structured in more detail below to emphasize the first research questions:

Focus group 20-30 years:

This group is composed mainly of young adults who spend half of their time working, while the other half is still used for studying. In general, it can be seen that young participants in the study are particularly concerned about the Employment Status dimension. The factor Reputation was frequently mentioned, as they want to make a good impression on superiors and other employees in throughout their young professional career. The main concern is that work behavior could be misinterpreted in video call applications. In particular, the employer could draw conclusions about an employee's concentration if, for example, a cell phone is briefly looked at or an e-mail is answered in parallel. For this reason, any secondary activities, such as other open programs, are often closed just before a video call. However, there are also concerns that, if necessary, private messages or information that are not intended for this conversation circle can be read. Responsibility towards data is another factor that was frequently mentioned. There is a concern that company data will be mismanaged, which could again cause the employee relationship to suffer.

After analyzing the data, it can be seen that concerns about control were also frequently named, which is reflected with previous literature (Malhotra et al., 2004, p. 339). Although the interviewed participants use video call applications daily in both the work and private spheres, they switch to other technologies, especially when communicating sensitive data. Existing literature also shows that, although new workplace communication tools have been implemented, e-mail traffic in particular is considered to be the most important one (Chory, Vela, & Avtgis, 2016, p. 26).

In private, young users of the studies show little privacy concerns. Young participants often use video call applications (e.g. FaceTime) to share general topics with their friends and family. It is known that young people have fewer privacy concerns (cf. Culnan et al., 1994; Smith et al., 2011, p. 999). This could result primarily from the fact that young people are more familiar with these communication methods. Only important documents (e.g. passwords) are also shared due to insufficient control by other communication tools. Concerns are expressed here that the data could be used for other purposes.

Focus group 30-40 years:

The second focus group has been in full-time employment for several years. Concerns about employment status are still mentioned, but to a lesser extent. Above all, the factor of company-internal improper access stands out in the frequency of naming. This factor has already often been an important factor/important dimension in other fields of research (e.g. Becker, 2018; Hong & Thong, 2013; Smith et al., 1996). Especially in the work context it is evident that applications like Microsoft Teams are also used for private conversations, where there are concerns that other employees or the company may see them during a call e.g. through screen sharing etc (Clarke, 1999, p. 25). This concern also follows the increase of virtual meetings. Moreover, the concern is that in the worst case, this could lead to dismissal.

Furthermore, the factor of application error is mentioned. The functionality of individual tools and functions is questioned and leads to concerns. The mute function of Zoom is questioned, and participants prefer to leave the room. There are also concerns about control, as communication through video call applications can be poorly tracked. The loss of data is therefore more likely, in the opinion of the users. For communication, this focus group (as well as the focus group 40+) mainly use the video call applications Zoom and Microsoft Teams. The Microsoft Teams application is used primarily for exchanging instant messages (which are increasingly private), while Zoom is used more for scheduled meetings and external customers. However, there is no general trend that privacy concerns are becoming more prevalent in one of the applications mentioned above.

There are also fewer concerns in the private sphere. This focus group explains this mainly stating the fact that they do not have to fear any consequences in their private life that they have in their professional life.

Focus group 40+:

Participants in this focus group have only recently become familiar with communication tools such as video call applications compared to their work careers. Interestingly, privacy concerns per se are hardly mentioned in the last focus group.

Instead, behavioral patterns emerge that allow conclusions to be drawn about concerns.

In the work context, the oldest participants in the study assume that sufficient security standards are provided by the company so that both personal and company data can be secured. Concerns are expressed that all communication is tracked, which brings the collection dimension to the center of attention. In addition, new technologies such as video call applications are seen as an additional challenge, since constant accessibility increases (i.e. performance tracking). In general, the issue of privacy is nevertheless very important for older participants.

In their private lives, they hardly ever use video call applications and clearly prefer to use the telephone or even personal contact. However, personal data as well as privacy issues in general are considered particularly important by older participants. There is a trend that a higher level of privacy regarding data leads the less usage of digital technologies. To underline the second research questions, the reasons for the differences in privacy concerns are investigated below.

Reasons for differences in privacy concerns:

In conclusion, privacy concerns are more apparent in the work domain than in the private domain. This is primarily attributable to the fact that private data must be protected more strongly than when the technologies are used privately. Due to the different relationships with various stakeholders, it is difficult to standardize who can access data in the workspace. In addition, data sharing as well as the issue of data privacy are questioned more often in work life. Concerns about the application are equally low in both areas. The context and the environment are decisive factors influencing concerns (Bansal & Zahedi, 2008; Smith et al., 2011, p. 1002). Nevertheless, it is apparent that privacy concerns are not increasing strongly due to the use of other digital communication applications. Interviewed participants do not feel monitored but rather appreciate the technical capabilities of the communication applications.

6. Implications and Future Research

This study has important theoretical and practical implications. The visualized structure of the thematic map shows the different privacy concerns for the use of video call applications in private and business settings. While there are certainly other factors that influence the concerns, this thematic map provides a good starting point. It indicates that already validated dimensions (e.g. Control, Awareness etc.) of established constructs can be applied to the context of video call applications. The results of this study can therefore contribute to the understanding of privacy concerns in digital communication and identify possible avenues for future research. For example, further research could verify the relationship between the factors developed and the dimensions of the thematic map in a quantitative study (cf. Becker, 2018, p. 3268). Relationships between concerns are already apparent and should be explored through quantitative correlations. Moreover, the results of this study could support efforts to formulate theories to reveal the meaningful interaction between privacy concerns and the perceived benefits and acceptance of communication technologies. The dilemma of using communication technology when transmitting confidential data and privacy concerns about reputational damage in the workplace due to increased transparency show that privacy in the workplace is an important area of research. Further literature should examine other factors of privacy concerns in different technology applications, such as email. The rise of remote work and home office regulations has led to an increase in merging of private and business life, which also raises privacy concerns regarding the working environment. In addition, there is the question of how employers deal with employee concerns and who the appropriate contact person within the company is.

The thematic map can serve as a practical guideline for providers to develop more privacy friendly video call applications in work and private life. This study also shows that control over one's own data is seen as the most important dimension regarding communication privacy concerns. Employers should ensure that employees have more certainty about their control over personal data. Transparency regarding which data is collected and to whom it is accessible should be increased. The implementation of security standards by both the application provider and the employer should be encouraged.

7. Limitations

An obvious limitation of this study was the small sample size of 18 participants who took part in focus groups. Nevertheless, care was taken to ensure that the three focus groups represented a large, diversified sample of the general population in terms of age (i.e., age range from 20-63 years). Moreover, attention was paid to an average group size of approx. 6 participants. Especially when interviewing emotionally charged topics, a group should not be too large in terms of size (Morgan, 1996, p. 146). The ability to facilitate a group-level discussion, which is a strong advantage of the collection method, is also one of its major limitations, because of the danger of dominant personalities controlling a group discussion (Becker, 2018, p. 3269). An attempt was made to include all participants equally in the discussion to avoid a one-sided bias. The first interview with the youngest focus group was conducted in English. Results of the focus group 30-40 years and 40+ had to be translated from German into English, which could potentially lead to changes in what was said. It became apparent that older participants were more comfortable discussing the emotional topic of privacy in their native language. Although the terminology of privacy research was explained at the beginning of each interview, older participants had difficulty understanding it. The result was a shift to other topics and the naming of privacy concerns in the online context.

Many of the questioned participants (12 out of 18 participants) work for the same company, so the number of dif-

ferent applications is limited. Nevertheless, in the selection of these participants, an attempt was made to find as many departments of this company as possible

All group interviews were carried out using the video call application Zoom, which partly disturbed the productivity of the interviews and thus the group dynamics due to technical problems. Nevertheless, it is recognized in literature that Zoom is a suitable medium for collecting qualitative data (Archibald et al., 2019).

Lastly, due to the use of different video call applications in the business as well as the private sector, a comparison of the privacy concerns regarding the application is not always justified.

8. Conclusion

This study attempted to answer two questions regarding the investigation of privacy concerns in the use of video call applications. Firstly, it aimed to find out how the privacy concerns of users of these technologies differ in the work context from the private context. Secondly, this paper wanted to discover the underlying cause for these differing concerns.

Focus group interviews were conducted to answer these questions. Participants were required to use video call applications in both business and personal contexts. The results of the qualitative research were presented visually using a thematic map. Users expressed great privacy concerns regarding the control of sensitive data. In addition, work behavior and employment relationships are becoming more transparent, which raises more concerns. Employees in particular try to protect private confidential data at work.

This paper presents one of the first exploratory findings in the field of privacy research in the workplace.

References

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*.

Archibald, M. M., Ambagtsheer, R. C., Casey, M. G., & Lawless, M. (2019). Using Zoom Videoconferencing for Qualitative Data Collection: Perceptions and Experiences of Researchers and Participants. *International Journal of Qualitative Methods*, *18*, 1609406919874596.

Bansal, G., & Zahedi, F. (2008). The Moderating Influence of Privacy Concern on the Efficacy of Privacy Assurance Mechanisms for Building Trust: A Multiple-Context Investigation. *ICIS 2008 Proceedings*, 7.

Becker, M. (2018). *Understanding Users' Health Information Privacy Concerns for Health Wearables*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS quarterly*, 1017–1041.

Bélanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245–270.

Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management*, *46*(1), 127–164.

Braun, V., & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165.

Buck, C. (2015). *App-Privacy as an Abstract Value–Approaching Contingent Valuation for Investigating the Willingness to Pay for App Privacy*.

Buck, C. (2018). *Beiträge Zur Untersuchung Der Informationellen Privatheit Im Rahmen Des Experiential Computing*.

Buck, C., & Dinev, T. (2020). Low Effort and Privacy–How Textual Priming Affects Privacy Concerns of Email Service Users. *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Budd, J. W., & Bhave, D. (2008). Values, Ideologies, and Frames of Reference in Industrial Relations. In *The Sage Handbook of IndustrialRelations* (pp. 92–112). London: Sage.

Budd, J. W., & Bhave, D. (2010). The Employment Relationship. In *Handbook of Human Resource Management* (pp. 51–70).

Chawla, A. (2020). Coronavirus (Covid-19) Zoom application Boon or Bane. *Available at SSRN 3606716*.

Chellappa, R. K., & Sin, R. G. (2005). Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, *6*(2-3), 181–202.

Chory, R. M., Vela, L. E., & Avtgis, T. A. (2016). Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. *Employee Responsibilities and Rights Journal*, *28*(1), 23–43.

Clarke, R. (1999). Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*, *42*(2), 60–67.

Connolly, R., & McParland, C. (2012). Dataveillance: Employee Monitoring & Information Privacy Concerns in the Workplace. *Journal of Information Technology Research*, *5*(2), 31–45.

Consumers-Union. (2008). *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy.* Retrieved 22-11-2020, from http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html

Culnan, M., Smith, H., & Bies, R. (1994). *Law Privacy and Organizations: The Corporate Obsession to Know V. The Individual Right Not to Be Known*. The Legalistic Organization.

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.

Epic. (2020). *Public Opinion on Privacy.* Retrieved 22-11-2020, from https://epic.org/privacy/survey/

Glaser, B. G., Strauss, A. L., & Strutzel, E. (1968). The Discovery of Grounded Theory; Strategies for Qualitative Research. *Nursing Research*, *17*(4), 364.

Gomez, J., Pinnick, T., & Soltani, A. (2009). Knowprivacy.

Hong, W., & Thong, J. Y. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, 275–298.

Jiang, Z., Heng, C. S., & Choi, B. C. (2013). Research Note–Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, *24*(3), 579–595.

Kagan, D., Alpert, G. F., & Fire, M. (2020). Zooming into Video Conferencing Privacy and Security Threats. *arXiv preprintarXiv:2007.01059*.

Kitzinger, J. (1995). Qualitative Research: Introducing Focus Groups. *BMJ*, *311*(7000), 299–302.

Krasnova, H., & Kift, P. (2012). Online Privacy Concerns and Legal Assurance: A User Perspective. *AIS SIGSEC WISP Workshop onInformation Security and Privacy*, 1–23.

Lacono, P., V. L. Symonds, & Brown, D. H. (2016). Skype as a Tool for Qualitative Research Interviews. *Sociological Research Online*, *21*(2), 1–12.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22-42.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (Iuipc): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355.

Margulis, S. T. (1977). Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues*, *33*(3), 5–21.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of social issues*, *59*(2), 243–261.

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does Sample Size Matter in Qualitative Research?: A Review of Qualitative Interviews in Is Research. *Journal of Computer Information Systems*, *54*(1), 11–22.

Morgan, D. L. (1996). *Focus Groups as Qualitative Research*. Sage Publications.

Morton, A. (2014). All My Mates Have Got It, So It Must Be Okay: Constructing a Richer Understanding of Privacy Concerns–an Exploratory Focus Group Study. In *Reloading Data Protection* (pp. 259–298). Springer.

Moshki, H., & Barki, H. (2014). *Individuals' It-Related Privacy Concerns: A Two-Phase Cognitive Model*.

Murphy, K. (2020). Why Zoom Is Terrible. *The New York Times*, *23*.

Myers, M. (2009). *Qualitative Research in Business & Management*. Sage Publications.

Nissenbaum, H. (2009). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Patton, M. Q. (1990). *Qualitative Evaluation and Research Methods*. SAGE Publications.

Pavlou, P. A. (2011). State of the Information Privacy Literature: Where Are We Now and Where Should We Go? *MIS quarterly*, 977–988.

Reith, R., Buck, C., Walther, D., Lis, B., & Eymann, T. (2019). *How Privacy Affects the Acceptance of Mobile Payment Solutions*.

Rössler, B. (2001). *Der Wert Des Privaten*. Suhrkamp Frankfurt am Main.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS quarterly*, 989–1015.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS quarterly*, 167–196.

Solove, D. J. (2005). A Taxonomy of Privacy. *U. Pa. L. Rev.*, *154*, 477.

Solove, D. J., & Hoofnagle, C. J. (2006). Model Regime of Privacy Protection. *U. Ill. L. Rev.*, 357.

Stewart, K. A., & Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, *13*(1), 36–49.

Stone, E. F., & Stone, D. L. (1990). Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms. *Research in Personnel and Human Resources Management*, *8*(3), 349–411.

Wagenseil, P. (2020). Zoom Security Issues: Here's Everything That's Gone Wrong (So Far). *Tom's Guide*, *11*.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 193–220.

Weiler, S., Matt, C., & Hess, T. (2019). Understanding User Uncertainty During the Implementation of Self-Service Business Intelligence: A

Thematic Analysis. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Westin, A. F. (1968). Privacy and Freedom. *Washington and Lee Law Review*, *25*(1), 166.

Wiederhold, B. K. (2020). *Connecting through Technology During the Coronavirus Disease 2019 Pandemic: Avoiding "Zoom Fatigue*". Mary Ann Liebert.

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, *12*(12), 1.

Xu, H., Teo, H.-H., Tan, B. C., & Agarwal, R. (2012). Research Note - Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services. *Information Systems Research*, *23*(4), 1342–1363.