Investigating Consumers' Offline Privacy Behaviors and their Online Equivalents

Seminar Paper

Aleksandar Bachvarov
Xueying Sun
Meng-Chun Chen

Degree Course: Information Systems, Economics Engineering
Matriculation Number: 1960367, 2381308, 2439449

Institute of Applied Informatics and Formal Description Methods (AIFB)

KIT Department of Economics and Management

Advisor:	Dr. Tobias Dehling
Supervisor:	Prof. Ali Sunyaev
Submitted:	January 29, 2024

Abstract

As the use of technology becomes increasingly ubiquitous in our daily lives, privacy concerns have become more prominent. This study aims to investigate the offline and online privacy behaviors of consumers to provide insights into how individuals protect their personal information in their day-to-day life. A qualitative research design was used, which involved conducting 39 semi-structured interviews, ensuring a heterogeneous sample, and 4 focus groups with participants knowledgeable in online technologies. The study identified a range of offline and online privacy behaviors, such as shredding documents, using strong passwords, and avoiding public Wi-Fi. The results also revealed that offline and online privacy behaviors are interconnected. The study's implications suggest that policymakers and businesses providers need to understand consumers' privacy behaviors to provide better protection for personal information. Future research can investigate the impact of contextual factors such as culture, age, gender, and personality on privacy behaviors and determine the effectiveness of different privacy behaviors in safeguarding personal information. Despite some limitations, such as small sample size and reliance on self-reported data, this research adds valuable insights to the literature on the privacy behaviors of consumers.

Contents

1 Introduction

Privacy is now a major concern in politics, society, and for individuals. Surveys report that 67% of internet users worldwide are more concerned about their online privacy than ever before [Vuleta, 2022]. However, managing personal information online is becoming increasingly difficult, and as a result, 79% of online users worldwide feel they have lost all control over their personal information [Vuleta, 2022, Choi et al., 2018]. Repeated consumer data breaches have given people a sense of futility, ultimately making them weary of having to think about online privacy [Choi et al., 2018]. Some internet users have given reasons for their privacy concerns: (1) Polls have found that most internet users are concerned about how websites handle their personal information [Wu et al., 2012]; (2) Online privacy policies are often not easy to understand, legally confusing, containing a lot of jargon, and requiring strong reading skills [McDonald et al., 2009].

Furthermore, Internet users have raised several points about these issues, arguing that: (1) 60% of users who provide false personal information say they would be willing to provide their real information if the site told them how it would be used [Westin, 1997]; (2) their privacy concerns could be reduced if websites provided privacy policies that were easy to understand [Wu et al., 2012]. Despite the widespread assumption in the field of Privacy Enhancing Technologies (PETs) that users can manage and protect their privacy in a conscious way, the reality is that they don't know what their behaviors mean, and 29% of users say they have never taken any action to protect their personal information [Poll, 2022]. The contradiction between assumptions and reality results in PETs leading to a method of protecting privacy that does not work well. Therefore, we propose the following questions in our study:

Q1: What privacy behaviors are people engaging in offline, and what are the expectations behind them?

Q2: What are the online equivalents of these privacy behaviors, and what are the expectations behind them?

Q3: How can the results improve the performance of PETs?

To answer these questions, we conducted two methods: interviews and focus groups. With our approach, we aim to gain more clarity on what privacy behaviors consumers are taking offline and online. These results can guide us in improving the performance of PETs to serve the privacy field and better protect the privacy of consumers.

The remainder of this paper is structured as follows: Section 2 provides a brief introduction to existing research on privacy, privacy behavior, and PETs. Section 3 gives an overview of our research methodology. Section 4 highlights the main results of our research approach. In section 5, we conduct a discussion to present the principle findings,

implications, limitations, and future research directions. Finally, in section 6, we end with a brief conclusion.

2 Background

2.1 Privacy and privacy protection

Warren and Brandeis defined privacy as "the right to be let alone" [Warren and Brandeis, 1989]. According to Ross, privacy is the ability and/or right to protect our personal secrets, the ability and/or right to prevent invading our personal space [Anderson, 2020]. Privacy can be understood as a quasi "aura" around the individual, which constitutes the limit between him/her and the outside world [Lukács, 2013].

Fischer-Hübner proposed four ways to protect privacy: protection by government laws; protection by privacy-enhancing technologies (PETs); self-regulation for fair information practise by codes of conduct promoted by businesses; privacy education of consumers and IT professionals [Fischer-Hübner, 1998].

In our research, we will further identify what privacy behaviors consumers will engage in to protect their behavior. At the same time, we will focus on how PETs can be improved to protect privacy.

2.2 Privacy Enhancing Technologies (PETs)

PETs are a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system [Van Blarkom et al., 2003]. After the pseudo-identity was established, newer PETs gave rise to a classification in seven principles: Limitation in the collection of personal data, Identification/authentication/authorisation, Standard techniques used for privacy protection, Pseudo-identity, Encryption, Biometrics and Audit ability [Van Blarkom et al., 2003]. PETs belong to a class of technical measures which aim at preserving the privacy of individuals or groups of individuals [Heurix et al., 2015]. PETs can help individual users control the amount of personal information they disclose in an online transaction [Seničar et al., 2003]. The goal of PETs is to restore the balance of power between the individual who wants to retain privacy and many actors in the online environment who want to gather personal information [Seničar et al., 2003]. Heurix also proposed the goal of PETs is to protect user identities by providing anonymity, pseudonymity, unlinkability, and unobservability of users as well as data subjects [Heurix et al., 2015].

A prerequisite for the development of PETs is to understand the privacy needs of consumers. Only a true clarity of consumer requirements and expectations for privacy can improve the performance of PETs.

3 Methodology

3.1 Interview

Qualitative interviewing is a flexible and powerful tool to capture the voices and the ways people make meaning of their experiences [Rabionet, 2011].

In this phase, we hoped to gain insight into the private behaviors that consumers would engage in offline.

In the first step, we first clarified the purpose and format of the interviews. The purpose of the interview is to explore offline privacy behaviors and find the expectations of these behaviors. We conducted semi-structured one-to-one interviews, i.e. after initially developing an interview guideline, the interview questions were adjusted accordingly as the interview progressed. The interview was initially assumed to last between 15-30 minutes. In the second step, we developed an interview guideline (see Appendix 1) and identified the interviewees, i.e. a heterogeneous sample (i.e. different ages, different occupations, different nationalities, different levels of education, etc.). In the third step, we conducted the interviews and recorded them through notes for subsequent analysis. At the same time, the specific questions of the interviews were gradually adapted as the interviews progressed. In the fourth step, we summarised and analysed the interview data to classify privacy behaviors, situations and expectations to provide the basis for the next stage of the research methodology.

3.2 Focus Group

In the second phase, we conducted four focus groups. We wanted to map the offline privacy behaviors obtained in the first phase to online privacy behaviors through focus groups, and to clarify the behavioral hidden expectations.

In the first step, we selected participants who had more knowledge about privacy and technology as the target group for this phase. In the second step, we brainstormed to note the online equivalents of the offline behaviors as well as their expectations. In the third step, the results were summarised and the online privacy behaviors were categorised.

4 Results

4.1 Interview Results

In this section, we report the findings of our study on consumers' offline privacy behaviors. Our sample consisted of 39 interviewees from diverse backgrounds and ages (see Table 4), with an average interview duration of 15-30 minutes. We identified more than 80 examples of offline privacy behaviors, each consisting of action, expectation and situation. Concretely, this resulted in 83 different actions, 21 expectations and 13 situations. Each behavior we categorized into one of three general groups: personal information, personal space or specific scenarios (see Tables 6-11).

The interviewees reported a variety of actions they take to protect their offline privacy, ranging from physical actions to verbal interactions. The most reported actions were "pretending to be on the phone", "pretending to not know the language", and "pretending to be in a hurry". These actions were often taken in situations where the interviewee wanted to prevent others from bothering them or taking their personal time. Other actions, such as wearing a mask or headphones, "taking more congested paths", or "using stairs instead of elevators", were reported to avoid attention or to protect personal space.

The expectation behind these actions varied, but most interviewees reported aiming to protect their personal information, space, and resources. Interviewees also reported wanting to avoid feeling uncomfortable, ashamed, or unsafe. Some interviewees reported incentivizing or expecting reciprocity from others to protect their privacy. Additionally, interviewees reported taking actions to protect their purchase records, shopping habits, and ideas.

The actions and expectations reported by interviewees were often situational. The most reported situations were on the street, in public places, on public transport, at work, at school, and at home. Other situations reported included shopping, withdrawing cash, paying, handling documents, travelling, interacting with technology, and communicating with people. Interviewees also reported taking actions to protect their privacy in dangerous situations, such as when staying in hotels or when lending their belongings. Some interviewees reported taking actions to protect their privacy while sharing or socializing with friends and family.

In summary, our study identified more than 80 examples of offline privacy behaviors taken by consumers in a variety of situations. These behaviors were reported to protect personal information, personal space, and resources, and to avoid feeling uncomfortable, ashamed, or unsafe. While the actions taken by interviewees varied, most were situational and were taken in public places, at work or school, or at home.

4.2 Focus Group Results

To gather information on the online equivalents of offline behaviors, we conducted focus groups with 11 participants divided into four homogeneous groups of 2-3 individuals each (see Table 5). The participants were all familiar with online technologies, which allowed for a more in-depth discussion of their online behaviors. During the 30–40-minute focus group sessions, we provided the participants with small sets of offline privacy behavior examples from the interview phase. We asked them to think of equivalent online behaviors that they are aware of or use to protect their digital (online) privacy. The participants provided around 65 examples, which can also be grouped into several categories based on their common themes (see Table 12).

In terms of privacy-enhancing technologies, participants reported using a variety of tools to block unwanted notifications and cookies. They also used VPNs, ad blockers, and popup blockers to prevent unwanted tracking and ads. To protect their accounts, participants reported using strong passwords, two-factor authentication, and password managers. Additionally, they used secure browsers, anti-virus software, and browser containers to protect their online activities.

Participants also reported avoiding certain online activities, such as not clicking on unfamiliar links, not accepting friend requests from strangers, and not posting their location or vacation plans online. They also mentioned the importance of using secure networks and not using public computers for sensitive activities.

Overall, the results of our focus groups suggest that there exists a wide range of online behaviors to protect personal information and resources. These behaviors range from simple actions like blocking notifications or not clicking on unfamiliar links, to more complex measures like using two-factor authentication and private search engines. As with offline behaviors, people's online privacy and security behaviors are shaped by their level of risk awareness and their perceived threats in the digital environment.

4.3 Offline behaviors and Online Equivalents

There are some offline behaviors that can be directly mapped to their online equivalents, while others may not have a direct correlation. For example, behaviors such as "pretending to not know the language" and "putting the spotlight on someone else" may not have a direct online equivalent, while "not sharing personal information" and "avoiding weak PINs" have clear online counterparts.

Additionally, some offline behaviors can have multiple online equivalents depending on the context. For instance, "pretending to be in a hurry" was mapped by participants to "using do not disturb mode", "using airplane mode" or "replying later". In other words,

an online behavior like using a VPN can be seen as equivalent to all offline behaviors, whose expectation involves “protecting information”. Consequently, the online examples are to be considered as equivalents more regarding the common expectation of multiple concrete offline actions as opposed to a "one on one" mapping between online and offline privacy behaviors.

Overall, while there is an overlap between offline and online privacy behaviors, they are not always directly comparable, and it is important to consider the context in which these behaviors occur.

5 Discussion

5.1 Principal Findings

5.1.1 Phase 1 - Interviews

After investigating first phase interview, we categorize the main private objectives of our interviewees which are personal space, personal identity and information and specific scenarios. Next step, we analyze the relative private behaviors and categorize them to the belonged categories. The findings of first phase interview as follows:

Personal Space:

In this category, generally, we analyze our interviewees that they have the private need to keep their personal space over certain distances. How do they behave so that they can keep their distance from others? They will create boundaries to protect their personal space. Furthermore, we explain the definitions of distance into two terms with more details - physical and mental distance in order to interpret the results more precisely. According to our respondents, they create physical distances to hold their personal zone, for example, work from home and avoid rush hour to decrease connections with others. The other example is to put their personal belongings in public transport to create distances and make them more comfortable to stay in their personal seat. On the other hand, people wear masks and headphones to set up invisible boundaries to avoid social contacts. Besides, switching languages is also part of protecting behaviors to escape attentions of their real intentions. Besides, they view their personal room as their personal zone, therefore, locking the door and closing windows are their protections for their privacy.

Personal Identity and Information:

In the second category, personal identity and information are concerned as personal extensions from our interviewees. Thus, to assure their positive personal identity and information is one of their great considerations. At the same time, they tend to evade any risks to damage their personal image. Other behaviors are also mentioned that using watermark is a safeguard for personal intellectual property. In the other case, the interlocutors type their judgements via messages instead of conversations when they discuss confidential topics. The meaning behind this behavior is they do not wish any exposure of their intent to others.

Specific scenarios:

We summarize the essential samples to specific scenarios which are indicated significantly from our interviewees. Firstly, monetary repercussions have most of concerns from our interviewees. Hiding personal monetary information is the top mission to keep their

personal momentous asset from danger. They cover their hand when they type their PIN numbers. In addition, we discover that purchase record is deemed as personal identity as well. As a result, some respondents do not apply for any membership card in order to unveil personal purchasing data, for instance. The reason is they expect service providers collect their personal purchase data for marketing use, so they doubt their purchase data in safe position. The second scenarios is avoiding ads. The most of interlocutors lean to ignore noises and interruptions, consequently they neglect the notifications from the Ads which they do not interest. Thirdly, taboo topics are seen as embarrassing themes which are relative to sexual orientation, personal diseases and real emotions. People tend to stop sharing and change to other acceptable subjects to evade the embarrassed feeling.

5.1.2 Phase 2 - Focus Groups

Before we started to interpret the results from second phase focus group, there are additional knowledge of Current Privacy Protection: Privacy-enhancing Technologies (PETs) must be acknowledged in order to map the second phase result .Privacy-enhancing Technologies (PETs) belong to a class of technical measures which aim at preserving the privacy of individuals or groups of individuals. Their goal is to protect user identities by providing anonymity, pseudonymity, unlinkability, and unobservability of users as well as data subjects [Heurix et al., 2015]. Some of the goals they have are [Bonawitz et al., 2022]:

Privacy Goal 1: Data Minimization

Privacy Goal 2: Data Anonymization

Privacy Goal 3: Transparency, Consent, and Verifiability

Additionally, the current aspect of information privacy also guides us to perceive the gaps between users and service providers. The current aspect of information privacy is as a social contract in 2016 due to diversity of users' information privacy needs

Year	Perspective	Cue
1890	Information privacy as a right [Warren and Brandeis, 1989]	Increasing prevalence of newspapers
1967	Information privacy as control [Westin and Solove, 2015]	Computerization of government databases
1996	Information privacy as commodity [Bonawitz et al., 2022]	Commercialization of information networks
2002	Information privacy as a set of related problems [Solove, 2002]	Absence of a universal conceptualization of information
2016	**Information privacy as social contract** [Martin, 2016]	**Diversity of users' information privacy needs**

Table 1: History of information privacy [Dehling, 2022]

We restate three same categories from first interview to map and frame the second phase interview results as follows:

(1) Personal Space:

Respondents use private tools, private router mode and VPN to establish private zone. The purpose is to construct a safe place in the digital world and avoid attention and interruption. To cite an instance, people tend to set up offline state (ex: MS team) even when they are online. There is a specific finding that people mentioned the reactions from social posts are more aggressive, so they attend to take extra care of what they posted, and they block the comment sections from the social media in order to evade humiliation.

(2) Personal Identity:

Interlocutors tend to fill only necessary and appreciate personal data which matches only the purpose of collection. The purpose is to prevent disclosure of unnecessary personal information. In the other case, people pretend even to create a fake account or fake personal information (ex: name, birthday...), because they do not trust the purpose of collection and their personal data will be kept in safety. The rest of the behaviors are to erase browser history, use code words instead key words to decrease attentions from others.

(3) Specific scenarios:

In monetary repercussions, the interesting finding is that people behave differently for the same purpose to maintain monetary safety. Some people are more willing to pay online because they trust the online payment system. However, some others are more likely to pay in cash because they consider cash is reducing the risks of leaking personal monetary

information. The second scenario is avoiding ads. Respondents set up online blockers (ex: ads, Cookie and Pop-up blockers) to reduce the disturbances. The third scenario is taboo topics which are relative to sex orientation, personal diseases, real emotions. People use private mode, VPN to care for viewing history. In other respects, some people use the code words instead of key words during conversation or messages, for instance, "happy water" replace with "alcohol".

5.1.3 Mapping Online to Offline behaviors

Category	Expectations	Offline behaviors	Online behaviors	Finding
Personal Space	Offline: Create boundaries	Physical: WFH	Private Mode, VPN	**Invisible online world***
	Online: Avoid interruption and humiliation	Mental: mask, headphones	No personal status (MS)	**Insecurity**
			Block comments	**Less social manners**
Personal Identity and Information	Protect personal thinking and identity	Texting instead of talking, Watermark	Erase browser history, Use fake account	**Lower ethic awareness of real self-identity in online world***
Monetary repercussions	Hide confidential information	No purchase record, cover pin	Use secure network, **Pay online vs. Pay in cash**	Good privacy protection in both
Advertisements(ads)	Avoid interruption	Ignore street ads	Use ad blockers	Systemic online protections
				Accept/reject cookies has the same expectation
Taboo topics	Avoid embarrassment	No sharing	Use private mode, **code words**	Good privacy protection in both

Table 2: Mapping Online to Offline behaviors

After investigating our first and second phase of interviews. If there are any equivalents between offline and online privacy behaviors? The answer is yes! There are some interesting findings from comparisons of both interviews. From the categories of personal space and personal identity and information, we detected that users have less trust, security and social manners and lower ethical awareness of real self-identification in the online world. It may be due to the isolation and lower awareness of virtual world, especially when users tend to do things in private mode and lock the door and window at the same time, people behave more real and have less concerns without social mask.

Moreover, we conclude that users' expectations for offline and online private preferences, we indicate that users have same needs in both areas as follows:

(1) Safety in personal space (ex: no interruption)

(2) Protect personal identity and information

(3) Protect personal concerns for specific scenarios

(4) No risk in leaking and hacking personal information

On the other hand, the interviewees response specifically that privacy protections are not always working. Due this finding we conclude the reasons as follows:

Users do not have enough privacy knowledge to judge the privacy protections

Users have doubts that service providers can manipulate protections

Hacking news lowers the users trust of IT security.

Every user has personal privacy priorities, so private preferences are different.

Afterwards, we map the results from second phase interviews and PETs to evaluate if there is any gap between the users' private expectations and the policy. Furthermore, we propose potential solutions for improving the gap of expectations from users and PETs as well.

5.1.4 Mapping Results to PETs

PET Goals	Users' Expectation	Matching	Reason/Concern
Data Minimization	Protect personal identity and information	✓	Users can make their own decisions well
Data Anonymization	No personal identity and information	✓	What does private mode really protect?
Transparency, Consent, Verifiability	**Easy to understand**	X	**Do not have enough knowledge to understand users' term**
			Trust issues: manipulation
			IT-security issues: news from hacking
Confidentiality of the goal (see suggestions)	**Data Confidentiality**	?	**No leaking and hacking**
New Goal (see suggestions)	**Protect personal preferences in certain topics**	?	**Protect personal concerns for specific scenarios**
			Personal privacy preferences are different

Table 3: Mapping Results to PETs

Data minimization: PETs are matching users' expectations which users believe they can control the willing to give personal data for certain purposes.

Data anonymization: PETs are matching mostly of users' expectations. The most of users use private mode as their private protection. However, when we ask more deeper of this question which is how much do they know about the private mode or what does exactly protect in private mode. All the answers are no.

Transparency, consent and verifiability: The most of users mentioned that they can not understand the users' terms. Secondly, users do not trust generally service providers which they believe service providers can manipulate the policy and make it hard to understand. At the same time, current hacking news lower their trust of IT security to the service providers.

Extensional goals: The additional suggestions are considered the gap of users' expectations and PETs which indicates users' needs and expectations are not satisfied yet that can be additional improvement to current policy.

Confidentiality: Users still have strong uncertainty of data leaking and hacking risks. As a result, the solutions of integration to the safer protections are urgent to improve and develop.

Personal preferences: Due the diverse concerns within topics, everyone has individual tolerances and opinions regarding various subjects. Therefore, it is not appropriate to set the policy for everyone in the same page, so we propose to add personal preferences in the policy.

5.2 Implications

After analyzing the results from both interviews, we have some suggestions that could help improve PETs' performance.

For internet users:

We recommend that users do not overestimate capabilities when they have any problems. Searching for professional help will be more practical for solutions which are provided by experts.

In the other side, to empower necessary knowledge is a powerful solution. Therefore, we recommend enhancing users to be capable and competent actors in digital work, for instance, online privacy education in order to improve their skills to solve the problems.

For service provider:

Make the users' policy, terms and agreements are easy to understand.

Open the channels to interact with users for feedback, help and emergency rescues. When users have any urgent problems, they know where to search for support from service providers.

For government:

Set up more online polices for avoiding online criminal, privacy and IT security Direct the way when users have problem and attacks to online polices. Police in the real world represent justice, more online police bring more trust from users and fulfill their IT security expectations.

5.3 Future Research

While this study has provided a valuable insight into the offline and online privacy behaviors of consumers, there is still much to be explored in this area. Future research could focus on:

Exploring the relationship between offline and online privacy behaviors: While this study has identified some offline privacy behaviors and their online equivalents, there is still a need to investigate how consumers' offline privacy behaviors influence their online privacy behaviors and vice versa.

Investigating the impact of contextual factors on privacy behaviors: This study has identified various situations in which consumers engage in privacy behaviors, but it has not explored the contextual factors that may influence these behaviors. Future research could investigate how factors such as culture, age, gender, and personality impact privacy behaviors.

Examining the effectiveness of privacy behaviors: While this study has identified various privacy behaviors that consumers engage in, it has only subjectively assessed the effectiveness of these behaviors in protecting consumers' privacy. Future research could explore more in-depth the effectiveness of different privacy behaviors in protecting consumers' privacy in various contexts.

Examining the impact of privacy regulations on privacy behaviors: This study has not explored the impact of privacy regulations on consumers' privacy behaviors. Future research could investigate how privacy regulations, such as the General Data Protection Regulation (GDPR [Voigt and Von dem Bussche, 2017]) and the California Consumer Privacy Act (CCPA [Goldman, 2020]), influence consumers' privacy behaviors.

Overall, there is still much to be learned about consumers' offline and online privacy behaviors, and future research in this area could help to inform policymakers, businesses, and consumers about how to protect privacy in an increasingly digital world.

5.4 Limitations

Although our study provides a comprehensive list of offline and online privacy behaviors, it is important to acknowledge some limitations. First, our sample size for the interviewees was limited to 39 individuals, which may not be representative of the broader population. Additionally, while efforts were made to ensure a diverse sample, it is possible that some groups may be underrepresented in our sample.

Second, the study relied on self-reported data from participants, which could be subject to bias or social desirability effects. Furthermore, the focus groups were composed of only

11 participants, which may limit the generalizability of our findings.

Third, our focus groups included only individuals who are familiar with online technologies. Thus, our results may not generalize to individuals who are less tech-savvy or have limited access to online resources.

Additionally, behaviors were grouped based on a general description of the participants' expectations. Future work can involve separation into more detailed categories based on the actions themselves, their purpose, meaning, impact, effectiveness or the situation in which they are performed.

Finally, while our study identified a range of offline and online privacy behaviors, we did not examine in-depth the effectiveness of these behaviors in protecting individuals' privacy. Further research is needed to determine which privacy behaviors are most effective and how they can be improved.

Despite these limitations, we believe that our study makes a valuable contribution to the literature on consumers' offline and online privacy behaviors and provides a solid foundation for future research in this area.

6 Conclusion

In conclusion, this study aimed to investigate the offline and online privacy behaviors of consumers, with the goal of identifying similarities and differences between these behaviors and exploring the factors that influence them. Through a mixed-methods approach involving in-depth interviews and focus groups, we collected data from a diverse sample of individuals.

Our results suggest that while there are some similarities between offline and online privacy behaviors, there are also important differences, such as the types of information that people are willing to share in each context. We also found that contextual factors, such as culture and personality, can have a significant impact on privacy behaviors. Furthermore, our findings suggest that many consumers engage in privacy behaviors in an attempt to protect their personal information, but that the effectiveness of these behaviors may vary depending on the context.

The implications of these findings are significant for businesses, policymakers, and consumers alike. By understanding the offline and online privacy behaviors of consumers and the factors that influence them, businesses can design better privacy policies and products that meet the needs and expectations of their customers. Policymakers can use this information to craft more effective privacy regulations that take into account the complex and nuanced nature of privacy behaviors. Finally, consumers can use this information to make more informed decisions about how they share their personal information both online and offline.

However, it is important to acknowledge the limitations of this study, such as the small sample size and the reliance on self-reported data. Future research could build on our findings by exploring the relationship between offline and online privacy behaviors, investigating the impact of contextual factors on privacy behaviors, examining the effectiveness of privacy behaviors, and examining the impact of privacy regulations on privacy behaviors. Such research could help to further inform policy and practice and protect privacy in an increasingly digital world.

Overall, this study provides a valuable contribution to the literature on consumers' offline and online privacy behaviors and highlights the need for further research in this area. By understanding the complexities of privacy behaviors, we can better protect the privacy rights of individuals and foster a more secure and trust digital environment.

7 Appendix

7.1 Interview Guideline

7.1.1 Opening statement of the interview

Hello, I am a student at KIT. I am doing a research on privacy and really appreciate your participation. This interview will be conducted mainly through some opinion questions and behavioral questions. The content of the interview will be kept strictly confidential! To ensure the validity of the interview, please answer each question truthfully, and if there are no questions, let's get started!

7.1.2 Interview dialogue

Dialogue section:

1. Can you think of a thing that you do when you are outside that protects your privacy in some way?

   Note: Answers will often include online and offline examples. Try to steer the conversation into the offline.

2. Let's consider **example of offline behavior**, for example, have you noticed something interesting that people do, or you do in such situations?

   Note: After the interviewee has no examples left, present them with some interesting behaviors from previous interview sessions.

3. Have you witnessed or can you think of similar things that people do in their daily lives?

4. What is it that people are trying to protect?

5. What are their expectations?

6. How effective is **example of offline behavior**, in your opinion?

7. Do you consider yourself more privacy-conscious person than the average consumer?

Interview steps:

1. Selecting the interview site
2. Select the subject
3. Take notes
4. Reflection and evaluation of the interview

Problems that may be encountered

1. Refusal of the interviewee to answer
2. Highly intrusive interview locations
3. Impatience of the interviewee during the interview
4. Interruption by a third party during the interview

7.1.3 Closing

Thank you for your time, wish you a good day!

7.2 Interview Participants

Ind.	Category	#	Ind.	Category	#	Ind.	Category	#
Age	<18	1	Job	Unempl.	1	Education	Professor	1
	18-25	13		Retired	3		Doctor	1
	23-35	16		School	1		Master	12
	45-55	6		Student	20		Bachelor	17
	70-80	2		IT	4		High school	3
	>80	1		Medical	3		Elem. School	1
Origin	Europe	10		Hospitality	1		Career Educ.	1
	Asia	19		Factory	4		Low Educ.	3
	South Am.	2		Insurance	1	Gender	Male	15
	Australia	1		Design	1		Female	24

Table 4: Information about interview participants

7.3 Focus Group Guideline

7.3.1 Participants Recruiting

1. Carefully recruited the people who have high IT security awareness
2. Similar types of people

7.3.2 Moderator Skills

1. Exercise mild unobtrusive control
2. Adequate knowledge of topic

3. Appears like the participants
4. Use purposeful small talk
5. Use pauses and probes

    "Would you explain further?”

    "Would you give an example?"

    ”I don’t understand."
6. Written notes during the interview
7. Control reactions to participants

    Verbal and nonverbal;

    Head nodding;

    Short verbal responses (avoid "that’s good", "excellent")
8. Use subtle group control

    Experts Dominant talkers;

    Shy participants;

    Ramblers;

    Use appropriate conclusion
9. Make Conclusions

    Three-Step Conclusions :

    1. Summarize with confirmation,
    2. Review purpose and ask if anything has been missed,
    3. Thanks and dismissal

7.4 Focus Group Participants

# of groups	Participants per group	Total	Age	Education	Job
4	2-3	11	20-30	Bachelor	Student
				Master	Engineer

Table 5: Information about focus group participants

7.5 Offline Privacy behaviors

Protecting Personal Information		
Action	Expectation	Situation
Using fake name	Avoid fraud and bad actors	Interacting with people/technology
Not using full name	Avoid fraud and bad actors	Interacting with people/technology
Using pickup stations	Avoid being seen, Avoid discomfort	Shopping
Using screen protector	Prevent peeking	In public, At Work
Not using payback card	Protect purchase record	Shopping, paying
Not sharing address	Avoid fraud and bad actors	Interacting with people/technology
Not lending belongings	Avoid fraud and bad actors	In general
Not discussing health, status	Avoid fraud and bad actors	Interacting with people/technology
Paying loud music	Looking unapproachable	In public, At home
Pulling the curtains	Avoid being seen, Prevent peeking	At home, Hotels
Texting instead of talking	Safe communication, Avoid attention	In public, Taboo topics
Beware shoulder surfing	Prevent peeking, Avoid fraud	In public
Beware cameras/mics	Avoid being seen	Hotels, In public
Removing Information from trash	Avoid fraud and bad actors, Protect purchase record	In general
Speaking another language	Safe communication, Looking unapproachable	In public, Taboo topics
Speaking quietly	Safe communication, Avoid attention	In public, Taboo topics
Turning off devices	Safe communication, Avoid fraud	Interacting with people/technology
Putting stickers on cards	Avoid peeking, Avoid fraud	In general
Watermarking documents	Avoid fraud and bad actors	Handling documents
Entrusting only relatives with documents	Avoid fraud and bad actors	Handling documents
Separating important documents	Avoid fraud and bad actors	Handling documents

Table 6: Offline Privacy behaviors - Examples of protecting personal information

Protecting Personal Information		
Checking important documents alone	Avoid fraud and bad actors	Handling documents
Restoring factory settings	Not leaving information behind, Avoid fraud and bad actors	Interacting with technology
Ending sessions on devices	Not leaving information behind, Avoid fraud and bad actors	In public
Turning down screen brightness	Prevent peeking	In public
Keeping diaries/letters safe	Protect ideas, Protect personal emotions, Avoid feeling shame	In general

Table 7: Offline Privacy behaviors - Examples of protecting personal information, continued

Protecting Personal Space		
Action	Expectation	Situation
Sitting on outer seat	Prevent people from bothering you	In public
Blocking seat beside you	Prevent people from bothering you, Looking unapproachable	In public
Pretending to be asleep	Prevent people from bothering you, Looking unapproachable	In public, At home
Bringing own food/coffee to work	Avoid socializing	At work
Parking far away	Avoid attention	In public, At work
Avoid leaving on the (half)hour	Avoid attention, Avoid socializing	In public, At work
Working from home	Avoid socializing	At home
Meeting online	Avoid socializing	At home
Wearing mask, glasses, hoodie	Avoid attention, Avoid socializing	In public
Avoiding congested paths	Avoid Attention	In public, At work
Taking congested paths	Avoid Attention	In public
Using stairs, not elevator	Avoid socializing	In public, At work
Dressing appropriately	Avoid Attention	In public
Writing unrecognizably	Prevent peeking	At school
Express boundaries	Self growth, Avoid discomfort	In general
Doing something only at home	Avoid being seen	At home
Siting with back against the wall	Prevent peeking	In public, At work
Siting facing the wall	Avoid being seen	In public, At work
Locking the door	Physical safety	In public, At home, At work
Closing the windows	Physical safety	In public, At home, At work
Avoiding playing loud music	Avoid attention	In public, At home

Table 8: Offline Privacy behaviors - Examples of protecting personal space

Specific Scenarios (Money)		
Action	Expectation	Situation
Keeping money in inner pockets	Avoid bad actors	In general
Paying digitally	Avoid fraud and bad actors	Paying, Shopping
Paying in cash	Not leaving information behind	Paying, Shopping
Hiding withdrawn amount	Avoid fraud and bad actors	Withdrawing cash
Hiding PIN code	Avoid fraud and bad actors	Withdrawing cash, Paying
Hiding card information	Avoid fraud and bad actors	Withdrawing cash, Paying
Avoiding suspicious ATMs	Avoid fraud and bad actors	Withdrawing cash
Avoiding the little hours	Avoid fraud and bad actors	Withdrawing cash
Avoiding touristy exchanges	Avoid fraud and bad actors	In public
Using strong PINs	Avoid fraud and bad actors	In general
Using trusted platforms	Avoid fraud and bad actors	In general
Stalling the line	Incentivize behaviors, Reciprocity	Withdrawing cash, Paying
Not looking at peoples PINs	Incentivize behaviors, Reciprocity	In public
Not leaving wallet open	Avoid fraud and bad actors, Avoid peeking	In general
Not showing payment code in advance	Avoid peeking	Paying, Shopping
Not noting down the PIN	Not leaving information behind, Avoid fraud and bad actors	In general

Table 9: Offline Privacy behaviors - Examples of specific scenarios (money)

Specific Scenarios (Time)		
Action	Expectation	Situation
Pretending to speak on the phone	Looking unapproachable	In public
Pretending to not know the language	Looking unapproachable	In public
Pretending to be in a hurry	Looking unapproachable	In public
Wearing headphones	Looking unapproachable	In public, At work, school
Walking across the street	Avoid the 'spotlight', Avoid being seen	In public
Saying you're under 18	Looking unapproachable	In public, Taboo topics
Decline	Avoid socializing, Avoid discomfort	In general
Ignore	Avoid socializing, Avoid discomfort	In general

Table 10: Offline Privacy behaviors - Examples of specific scenarios (time)

Specific Scenarios (Other)		
Action	Expectation	Situation
Keeping lights on during absence	Protect resources, Avoid fraud and bad actors	At home, At work
Removing shoes from front door	Avoid attention	At home
Putting male shoes at the door	Physical safety, Avoid fraud and bad actors	At home
Using inside references	Safe communication	In general
Leaving fingerprints, hair	Physical safety	In public, In danger
Not sharing sexual orientation	Protect emotions	In general
Putting the spotlight on someone else	Protect emotions, Avoid attention, Protect ideas, Avoid discomfort	In general
Avoiding showing real emotion	Protect emotions, Protect ideas, Avoid discomfort	In general
Taking personal time	Self growth, Protect emotions	In general
Wearing earplugs	'Disconnect'	In general
Ordering two meals	Physical safety, Avoid fraud and bad actors	At home

Table 11: Offline Privacy behaviors - Examples of specific scenarios (other)

7.6 Online Equivalents

Online Privacy behaviors	
Block notifications	Not using the same password
Not clicking	Using strong password
Previewing the message	Multi-Factor-Authentication
Replying later	Always logout
Ignoring Message	End app sessions
'Do Not Disturb' mode	Beware public computers, wifi
'Airplane' mode	Beware suspicious links
VPN	Use secure browser
Ad blocker	Disable default tracking settings
Reject cookies	Check authenticity of website
Accept cookies	Burner card, mail, account
Close pop-ups	Mode for hiding phone number
Change status (e.g. busy)	Not accepting strangers in social media
Paying subscription	Remove tags from pictures
Buying app	Avoid social media
Blocklist for emails	Fill only required fields
Cancel personalized recommendations	Single-Sign-On
Browser plug-ins	Use work laptop for work
Multiple accounts	Avoid "remember password"
Pop-up blocker	Cold storage
Forward and listen voice messages	Private search engine
Erazing browser history	Self-hosting
Private router	Update IoT devices
Delete cookies	Update Software regularly
Password manager	Use giftcards
Anti-virus Software	Use PayPal, Klarna
Browser Containers	Use cryptocurrency
HTTPS instead of HTTP	Use trusted platforms
Private browser mode	Block comment section
Posting pictures with delay	Set profile to private
Not posting when on vacation	Curated posting
Not posting location	One-time-view message
E2E encrypted messaging	

Table 12: Online Privacy behaviors

References

[Anderson, 2020] Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

[Bonawitz et al., 2022] Bonawitz, K., Kairouz, P., Mcmahan, B., and Ramage, D. (2022). Federated learning and privacy. *Communications of the ACM*, 65(4):90–97.

[Choi et al., 2018] Choi, H., Park, J., and Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81:42–51.

[Dehling, 2022] Dehling, T. (2022). Cii lecture session-01.

[Fischer-Hübner, 1998] Fischer-Hübner, S. (1998). Privacy and security at risk in the global information society. *Information Communication & Society*, 1(4):420–441.

[Goldman, 2020] Goldman, E. (2020). An introduction to the california consumer privacy act (ccpa). *Santa Clara Univ. Legal Studies Research Paper*.

[Heurix et al., 2015] Heurix, J., Zimmermann, P., Neubauer, T., and Fenz, S. (2015). A taxonomy for privacy enhancing technologies. *Computers & Security*, 53:1–17.

[Lukács, 2013] Lukács, A. (2013). A munkavállalók személyiségi jogainak védelme, különös tekintettel a munkahelyi kamerákra. *DE IURISPRUDENTIA ET IURE PUBLICO: JOG-ÉS POLITIKATUDOMÁNYI FOLYÓIRAT*, 7(2):Terjedelem–32.

[Martin, 2016] Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of business ethics*, 137:551–569.

[McDonald et al., 2009] McDonald, A. M., Reeder, R. W., Kelley, P. G., and Cranor, L. F. (2009). A comparative study of online privacy policies and formats. In *Privacy Enhancing Technologies: 9th International Symposium, PETS 2009, Seattle, WA, USA, August 5-7, 2009. Proceedings 9*, pages 37–55. Springer.

[Poll, 2022] Poll, T. H. (2022). Norton cyber safety insights report: Special release – online creeping.

[Rabionet, 2011] Rabionet, S. E. (2011). How i learned to design and conduct semi-structured interviews: an ongoing and continuous journey. *Qualitative Report*, 16(2):563–566.

[Seničar et al., 2003] Seničar, V., Jerman-Blažič, B., and Klobučar, T. (2003). Privacy-enhancing technologies—approaches and development. *Computer Standards & Interfaces*, 25(2):147–158.

[Solove, 2002] Solove, D. J. (2002). Conceptualizing privacy. *California law review*, pages 1087–1155.

[Van Blarkom et al., 2003] Van Blarkom, G., Borking, J. J., and Olk, J. E. (2003). Handbook of privacy and privacy-enhancing technologies. *Privacy Incorporated Software Agent (PISA) Consortium, The Hague*, 198:14.

[Voigt and Von dem Bussche, 2017] Voigt, P. and Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676):10–5555.

[Vuleta, 2022] Vuleta, B. (2022). 18 chilling privacy statistics.

[Warren and Brandeis, 1989] Warren, S. and Brandeis, L. (1989). The right to privacy. In *Killing the Messenger*, pages 1–21. Columbia University Press.

[Westin, 1997] Westin, A. (1997). Privacy and american business study. *Retrieved online November*, 1:2010.

[Westin and Solove, 2015] Westin, A. and Solove, D. (2015). *Privacy and Freedom*. Ig Publishing.

[Wu et al., 2012] Wu, K.-W., Huang, S. Y., Yen, D. C., and Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. *Computers in human behavior*, 28(3):889–897.

Assertion

Ich versichere wahrheitsgemäß, die Arbeit selbstständig verfasst, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde sowie die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet zu haben.

Karlsruhe, January 29, 2024 VORNAME NACHNAME