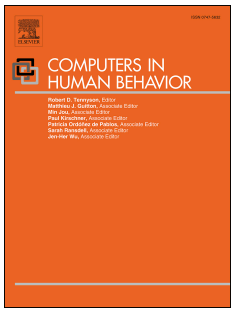

How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs

Verena Distler, Carine Lallemand, Vincent Koenig

PII: S0747-5632(19)30446-7

DOI: https://doi.org/10.1016/j.chb.2019.106227

Reference: CHB 106227

To appear in: *Computers in Human Behavior*

Received Date: 18 January 2019

Revised Date: 20 December 2019

Accepted Date: 21 December 2019

Please cite this article as: Distler V., Lallemand C. & Koenig V., How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs, *Computers in Human Behavior* (2020), doi: https://doi.org/10.1016/j.chb.2019.106227.

Credit author statement

Verena Distler: Conceptualization, Methodology, Writing - Original Draft, Writing - Review & Editing, Visualization
Carine Lallemand: Conceptualization, Methodology, Supervision, Funding acquisition
Vincent Koenig: Conceptualization, Methodology, Supervision, Funding acquisition

How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of the Acceptance of Privacy Trade-Offs

Verena Distler (corresponding author)
Verena.distler@uni.lu [a]

University of Luxembourg
Human-Computer Interaction Research Group
11 Porte des Sciences
Esch-sur-Alzette
Luxembourg

Carine Lallemand [a,b]
Carine.lallemand@uni.lu

Vincent Koenig [a]
Vincent.koenig@uni.lu

[a] Human-Computer Interaction Research Group, University of Luxembourg, Esch-sur-Alzette, Luxembourg
[b] Department of Industrial Design, Eindhoven University of Technology, Eindhoven, Netherlands

Declarations of interest: none

How Acceptable Is This? How User Experience Factors Can Broaden our Understanding of the Acceptance of Privacy Trade-Offs

ABSTRACT

Privacy is a timely topic that is increasingly scrutinized in the public eye. In spite of privacy and security breaches, people still frequently compromise their privacy in exchange for certain benefits of a technology or a service. This study builds on both technology acceptance (TA) and user experience (UX) research in order to explore and build hypotheses regarding additional dimensions that might play a role in the acceptability of privacy tradeoffs that are not currently accounted for in TA models. Using four scenarios describing situations with potential privacy trade-offs, we conducted a focus group study with 8 groups of participants (N=32). Our results suggest that factors influencing privacy trade-offs go beyond existing TA factors alone. A technology's perceived usefulness plays an important role, as well as dimensions related to context, previous experiences, perceived autonomy and the feeling of control over the data being shared.

AUTHOR KEYWORDS

Privacy trade-offs, User Experience, technology acceptance, qualitative methods.

1. INTRODUCTION

Technologies nowadays are able to perform complex tasks in most areas of people's lives, and many of these tasks may impact users' privacy. Privacy is defined as the ability of individuals to maintain control of their personal information (Westin, 1968). Privacy also relates to the notion of voluntariness, referring to the type of information about one's self or one's association that a person must reveal to others, under which circumstances and with which protections (Mason, 1986). The matter has indeed gained high topicality and public attention. Privacy initiatives such as the General Data Protection Regulation (GDPR) in the European Union aim at improving the regulatory landscape and establish, amongst other measures, the principle of "privacy by design".

When confronted with technologies, users' privacy behavior regularly reflects conscious or unconscious decisions on whether they accept privacy trade-offs, which involve sharing some level of personal data in exchange for using a product or service (Rainie & Duggan, 2015). While technology acceptance models offer a framework for studying acceptance, they have shortcomings such as the absence of psychological needs and negative emotions. Moreover, while factors about users, systems, tasks and organization context are widely recognized as important, many papers on technology acceptance do not address them (Hornbæk & Hertzum, 2017).

Our research leads to the following contributions:

- It adds to knowledge on factors influencing the acceptability of privacy trade-offs and gives insight into the non-instrumental aspects affecting acceptance of privacy-relevant technology, including autonomy, control, context-related factors. Thereby, it helps addressing the lack of non-pragmatic aspects (e.g., hedonic aspects, psychological needs, values) as those offered by UX frameworks, in the majority of acceptance models.
- It describes implications for the design of privacy-relevant systems.

1.1. Technology Acceptance Models

Technology acceptance can be defined as the judgement, attitude and behavioral reactions toward a product (Schade & Schlag, 2003). Technology acceptance models aim at explaining users' intention to use a system, mostly as a result of perceived usefulness (similar to performance expectancy) and perceived ease of use (similar to effort expectancy). These factors are at the basis of the first technology acceptance model (TAM) developed by Davis (1985), which has been extensively used and adapted to numerous contexts. Other influencing factors were introduced in later models, such as social influence. The UTAUT (unified theory of acceptance and use of technology (Venkatesh, Morris, Davis, & Davis, 2003)) hence describes behavioral intention to use a system as dependent on performance expectancy, effort expectancy and social

influence. In its updated version UTAUT2 (Venkatesh, Thong, & Xu, 2012), three new constructs, specific to consumer adoption, were introduced: hedonic motivation, price value and habit.

Application areas of acceptance models include for instance smart home technologies (Paetz, Becker, Fichtner, & Schmeck, 2011), social media (B. C. F. Choi & Land, 2016), health care records (Angst & Agarwal, 2009; Egea & González, 2011) or online tax (Wu & Chen, 2005).

1.2. Distinguishing User Experience and Usability

Usability traditionally focuses on "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" (ISO 9241-11). User Experience (UX), on the other hand, takes a broader approach in which task performance is put into perspective with additional aspects, including emotive, subjective and temporal factors of UX, going beyond instrumental facets (Hassenzahl & Tractinsky, 2006). The subjective meaning of an experience, emotional aspects (Desmet & Hekkert, 2007) as well as the context within which the interaction occurs (e.g., organizational/social setting, voluntariness of use, etc.) are within the scope of UX (Hassenzahl & Tractinsky, 2006). While usability is per se is goal-oriented, UX as a concept can also entail experiences with no performance expectations. Hassenzahl (2008) describes this multifactorial nature of UX using a distinction between instrumental (or "pragmatic") qualities and non-instrumental (or "hedonic") qualities of experience.

1.3. Links Between Technology Acceptance Models and User Experience

Pragmatic, or instrumental, quality describes a "product's perceived ability to support the achievement of do-goals" (i.e. tasks) (Hassenzahl, 2008) Hedonic quality refers to a product's perceived ability to support the achievement of "be-goals", such as "feeling safe" or "feeling competent" for instance (Hassenzahl, 2008). UX research also takes into account emotional, subjective and temporal aspects of interaction (Hassenzahl & Tractinsky, 2006),

It has been suggested that hedonic motivation might be a critical factor influencing behavioural intention in consumer-based contexts (Venkatesh et al., 2012). Human needs are are considered drivers of positive experiences (Hassenzahl, 2008; Sheldon, Elliot, Kim, & Kasser, 2001). The most relevant psychological needs have been narrowed down to autonomy, competence, security, relatedness, popularity, stimulation and security (Hassenzahl, 2008; Sheldon et al., 2001). The need for security is defined for instance as "feeling safe and in control of your life rather than feeling uncertain and threatened by your circumstances" (Sheldon et al., 2001). The fulfilment of psychological needs can be measured using a standardized questionnaire (Sheldon et al., 2001), and methods for qualitative assessment have been developed as well (Lallemand, 2015). Recent studies have applied psychological needs theories to the context of security and privacy (Distler et al., 2019; Kraus, Wechsung, & Möller, 2016, 2017).

It is important to stress that there are overlaps between UX and acceptance models. The TAM (Davis, 1985) for instance includes perceived usefulness (utility as defined by Shackel & Richardson (1991)) and perceived ease of use (similar to usability as defined by ISO 9241-11), and adaptations of the existing models to various contexts include some hedonic aspects (Al-Sharafi, Arsha, Abu-Shanab, & Elayah, 2016; Osswald, Wurhofer, Trösterer, Beck, & Tscheligi, 2012) such as perceived security, perceived safety or self-efficacy. Other extensions of the TAM have found that trust has a positive effect on behavioral intention to use, while usefulness, security and privacy perceptions influenced trust (Al-Sharafi et al., 2016; Venkatesh & Bala, 2008). Acceptance models thus partially cover certain mostly pragmatic UX factors, whereas other UX constructs such as psychological needs fulfilment are not yet included (Hornbæk & Hertzum, 2017), even though a strong tendency on their importance exists (Hassenzahl et al., 2013; Hornbæk & Hertzum, 2017).

1.4. The Acceptability of Privacy Trade-Offs

Privacy trade-offs can be defined as circumstances under which people would "share personal information or permit surveillance in return for getting something of perceived value." (Rainie & Duggan, 2015).

The acceptability of compromising one's privacy in exchange for certain advantages has been studied under various angles. The theory suggests that people's intention to disclose personal information depends on a privacy calculus, in which competing factors are assessed and users try to maximize the positive and minimize the negative consequences (Wottrich, van Reijmersdal, & Smit, 2018). The privacy calculus takes into account perceived privacy risk, privacy concerns, personal internet interest and internet trust (Dinev & Hart, 2006). This model has since been used in the context of social networks (Dienlin & Metzger, 2016; Krasnova, Veltri, & Günther, 2012), mobile devices (Keith, Thompson, Hale, Lowry, & Greer, 2013) and ecommerce (Luo, Li, Zhang, & Shim, 2010).

Some studies have also looked at discrepancies between user attitude and their actual behavior, a phenomenon called the privacy paradox (Norberg, Horne, & Horne, 2007), challenging the assumption that privacy-related decision-making is purely rational (Acquisti & Grossklags, 2005; Tsai, Egelman, Cranor, & Acquisti, 2011).

However, a large amount of factors play a role when studying privacy trade-offs. For instance, Rainie and Duggan (2015) studied the acceptance of privacy trade-offs in six different scenarios. Each scenario introduces the possibility of using a new technology offering certain advantages, which at the same time might also create a privacy risk. Participants' acceptance depended on a number of factors, such as trust in the company offering the deal, what happens to the data after it is collected and how long the data are retained. Both the conditions of a trade-off, as well as the circumstances of the participants' lives play a role. The potential availability of data to third parties was also a consideration.

In summary, technology acceptance models assess users' intention to use a system through factors such as performance and effort expectancy. The inclusion of non-pragmatic User Experience factors, such as psychological needs, into acceptance models has been considered relevant (Hornbæk & Hertzum, 2017) and the consciousness and rationality of privacy trade-offs has been challenged. There is thus a strong rationale to include factors that are not based on rationality, again underlining the relevance of UX for this topic. More research is therefore needed on the reasons which influence users' acceptance of privacy trade-offs in different contexts, investigating the influence of both acceptance and UX factors.

2. RESEARCH OBJECTIVES

Users sometimes accept certain privacy-related shortcomings in exchange for potential benefits of a technology. It is currently unclear whether technology acceptance models can be directly applied to privacy- and security-critical contexts, or whether important factors would be missing. The objective of this study is thus to explore and build hypothesis on additional dimensions which impact the acceptability of privacy-relevant technologies, thereby taking an interdisciplinary approach that contributes to bridging UX and TA models. Most TA models currently lack links to UX models. In particular, various hedonic qualities of experience are missing, such as psychological need fulfilment, which can provide a way of understanding the motivations behind the aims of use, or social factors (Hornbæk & Hertzum, 2017).

Our study addresses the following research question:

- To what extent can we use UX factors to complement technology acceptance models to be more applicable to the context of privacy-related technologies?

3. METHODOLOGY

We used a qualitative approach in order to obtain in-depth insights helping us understand to what extent UX factors can be used to complement technology acceptance models in the context of privacy-relevant technologies. A qualitative approach is well suited in this context to generate hypotheses on whether additional dimensions might be missing in the existing acceptance models. Qualitative studies also allow researchers to acquire an understanding of the situations in which technology is used (Blandford, Furniss, & Makri, 2016) and to discern the meaning people assign to processes and structures in their lives (Miles, Huberman, & Saldana, 2014). We used focus groups because group interactions force participants to question their beliefs and eventually to argument in order to defend their opinions (Krueger & Casey, 2014). To do so, they often rely on personal stories and also describe the values underlying their viewpoints. In addition, focus groups allow for factors outside the classical scope of acceptance models to show their relevance.

3.1. Participants

Thirty-two participants (17 men, 15 women) from different cultural and socioeconomic backgrounds participated in focus groups discussions. We created eight groups of a manageable size: two IT-literate expert groups, two student groups with non-IT related majors, and four groups of the general population. Experts and non-experts participated in separate groups to avoid experts influencing the other participants' opinions. The expert groups were recruited using the authors' professional networks while the student groups were recruited at the university. Recruitment within the general population was conducted using social network groups of local municipalities. Participants received a financial compensation. The average age of our participants was 33 years (Min=19, Max=55). Our sample covered various educational backgrounds. The participants had a multitude of nationalities (anonymized).

3.2. Procedure

We conducted eight focus groups, of which four took place in a face-to-face setting and four online, allowing us to reach people beyond the geographical area of the university. Each group comprised 4 to 5 participants who did not know each other. The sessions were administered in January 2018, during a single week in order to reduce the potential impact of a privacy-related information that would have spread in the news. The face-to-face focus groups took place at the university, each session lasting about an hour. For the online focus groups, we decided to opt for Facebook, a tool that our participants were familiar with. We gave them the possibility to create a fake Facebook account in case they did not want their real name to appear in the focus group discussion, but only one participant used this possibility. The focus group discussion took place

in a “private Facebook group”, so that only the facilitator and the participants could access the discussion. All focus groups (online and offline) were conducted by the same facilitator who was a UX expert, working in the field of usable security, and trained in qualitative methods. This ensures high consistency with regards to the facilitations style and adherence to ethics standards.

Participants were presented a selection of technology use scenarios derived from Rainie and Duggan’s report (2015). Given that we adopted a focus group approach, we chose to remove two of the scenarios used in their original study so we would have sufficient time to have an in-depth discussion for all scenarios without exceeding the one hour limit. The four scenarios we selected clearly described each situation with its advantages and disadvantages (Table 1). We selected one scenario (“free social media”) describing a technology that is broadly used already, while the remaining three scenarios are still rather innovative. All of the scenarios describe a potential situation in which a technology could provide some benefits in exchange for the user sharing different types of data. In the following, we will refer to acceptability of these scenarios (the prospective judgement toward a technology which has not been experienced yet (Schade & Schlag, 2003)) rather than acceptance, given that the described technologies have not yet been used by our participants, at least under the specific conditions mentioned.

Participants first commented on each scenario individually by writing down the pros and cons. Once all participants had written down their opinions on each scenario individually, a group discussion on the acceptability of the described technologies followed. Participants were instructed to comment on the reasons why they thought a scenario was acceptable or unacceptable, and to discuss various opinions. In order to get a rich picture of the factors influencing privacy-related acceptability, participants were not constrained to only discussing privacy-related issues, but their opinions on the acceptability in general, privacy concerns were discussed only if they emerged naturally. The facilitator ensured that all participants contributed to the discussion and shared their viewpoint.

3.3. Qualitative Content Analysis Process

A transcription of all focus group data was prepared to facilitate further analysis. The qualitative analysis process broadly followed Braun and Clarke’s (2006) thematic analysis approach. They describe six phases of thematic analysis, starting with (1) familiarisation with the data, (2) a generation of initial codes and (3) searching for themes. After, (4) themes are reviewed and then (5) defined and named. Lastly, (6) the sixth step is the creation of the report. For the present study, after transcribing and familiarising themselves with the data, the first author generated initial codes using a bottom-up approach and searched for themes. The author then organized the themes in an affinity diagram, in order to map them with regards to the factors known from acceptance and UX frameworks. At this point, the other authors reviewed the themes and their links to the theory as suggested by the first author. The authors then discussed any disagreements and agreed on a final set of themes and their links to acceptance and UX theory.

Scenario	Description
Office surveillance cameras	"Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the thcompany wishes to retain it, and could be used to track various measures of employee attendance and performance."
Sharing health information	"A new health information website is being used by your doctor's office to help manage patient records. Your participation would allow you to have access to your own health records and make scheduling appointments easier. If you choose to participate, you will be allowing your doctor's office to upload your health records to the website and the doctor promises it is a secure site."
Smart thermostat	"A new technology company has created an inexpensive thermostat sensor for your house that would learn about your temperature zone and movements around the house and potentially save you on your energy bill. It is programmable remotely in return for sharing data about some of the basic activities that take place in your house like when people are there and when they move from room to room."
Free social media	"A new social media platform is being used by your former high school to help manage communications about a class reunion. You can find out the basic information about the reunion over email, but your participation on the social media site would reconnect you with old friends and allow you to communicate more easily with those who are attending. If you choose to participate, you will be creating a profile using your real name and sharing a photo of yourself. Your access to the service is free, but your activity on the site would be used by the site to deliver advertisements it hopes will be appealing to you."

Table 1: Description of the scenarios from Rainie and Duggan (2015) used in the present study (French translation available in the supplementary material).

4. RESULTS

In the following, participant codes are assigned to the verbatims. Participants 1-16 took part in face-to-face focus groups, participants 17-32 in online focus groups (Expert groups: P1-P4 and P17-P21, Student groups: P5-P8 and P22-P25, General population: P9-P16 and P26-P32).

4.1. Office Surveillance Cameras Scenario

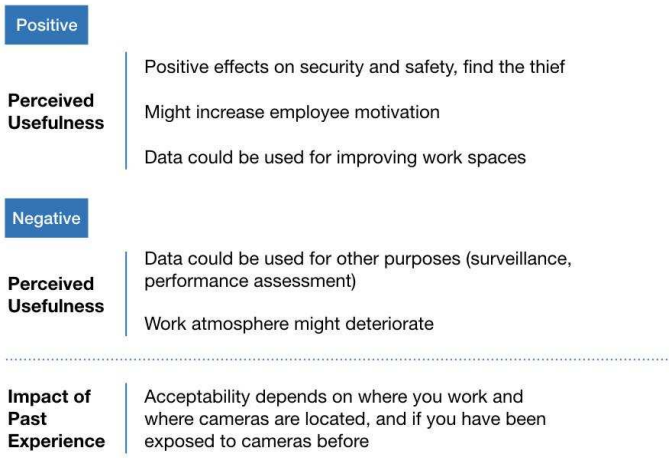

Figure 3: Most used arguments in favour of and against acceptability of the scenario "office surveillance cameras".

Perceived Usefulness

On the positive side (Figure 3), participants stated that the office cameras might improve security and safety, and that they might help find the thief (as presented in the scenario). A few of them also argue that office cameras might positively impact employee motivation for instance by discouraging non work-related activities: *"Company controls employees, so no free-riders are watching Netflix during the working time." (P6, Student)*

Another positive aspect mentioned, perhaps more surprising as it does not relate to any part of the scenario, was that data about office occupancy and flow of people could be used as a basis for improving the design of work spaces: *"In a good way, it could be used to improve work experience, and the design of work spaces." (P1, Expert)*

Negative aspects (Figure 3) were overall prominent in group discussions about this scenario, with participants fearing that data could be used for other purposes than security, such as surveillance of employees or performance assessment. These uses were perceived as intrusive, and some participants thought that security was mainly used as a pretext to introduce employee surveillance.

"It is not acceptable because it goes beyond the initial objective of finding the thief, which I am ok with, but if it is also for monitoring people [...] it goes beyond the acceptable, especially if the cameras use facial recognition." (P12, General population)

"I would feel like the company uses a phony reason in order to execute a plan that aims at monitoring and judging employees without their knowledge." (P19, Expert, in the context of surveillance cameras)

"It is not only about how we work, but also what we eat for lunch and who we are talking to." (P7, Student)

Lastly, participants indicated that cameras would deteriorate the work atmosphere and end up having negative consequences on the productivity of employees:

"It creates an atmosphere of mistrust and of "big brother is watching you." This is bad for the work atmosphere too, so I am not sure that the objective of performance will be reached by this mean." (P15, General Population)

Context

Most of the participants agree that the acceptability of these surveillance cameras depends on the type of work done, and the location of the cameras:

"*There are certain places where it is required [...], like hotels, sports centers, something like this." (P7, Student)*

"It is not acceptable in office corridors or office rooms. Entrances and reception lobby is fine." (P23, Student)

Impact of past experiences

Participants having worked in specific places, such as shops or hotels, declared being used to it and therefore having less issue with the acceptability of the scenario: *"But for me, I am fine. I mean I was always working in a company where there were cameras everywhere, because I was working in a hotel and we had to be protected, so I am fine with that." (P6, Student)*

4.2. Sharing Health Information Scenario

Figure 4: Most used arguments in favour of and against acceptability of the scenario "health information".

Perceived usefulness

A majority of participants thought that the increased efficiency when taking appointments and improved communication between doctors were positive aspects of this scenario (Figure 4). Another argument, mentioned several times, in favour of using the health information platform was that online banking worked: *"We are slowing down the evolution of the [e-health record] system because of security questions, which can be managed. The banks are doing it well!" (P19, Expert), "I feel like bank accounts are more secure" (P9, General Population).* This led to discussions about the sensitivity of bank data as compared to health data: *"It is the same thing with bank account data. I prefer that someone knows my medical data rather than my bank account." (P10, General Population), "Bank data is not as sensitive as health data." (P32, General Population).*

Eventually, a question that also occupied our participants was the added value of sharing the data. Some found that it might be preferable to only enable patients to book appointments online, without in return obliging them to share their medical data on the platform.

Perceived Control and Autonomy

Participants appreciated that patients would have more control over their medical data. The importance of free consent was emphasised by participants, who acknowledge the fact that using the health information platform was not mandatory in the scenario. One should *"not be obliged to enrol" (P11, General Population)* and *"Personal consent is required." (P24, Student).*

A considerable number of participants were concerned about what happened to their data. They wondered who could gain access to it and were concerned about hacking*: "Even if it is secure, there will always people who can [hack the health data], there is always someone who is smarter. They can crack anything anyhow." (P13, General Population)*

Some mitigated that fear by stating that the current medical system might already be flawed: *"Well, there are IT security flaws, that's what I noticed, but at the same time [at the moment] I'm pretty sure that my data is already digitized and stored on a server somewhere and I'm not even sure where they are [...]." (P15, General Population)*

On the technical side, some expert participants also found that there was not enough information on the security mechanisms that were used to make the platform secure. This expert would for example double check how secure the platform is: *"If my doctor "promises" that the site is secure, I will not take his word for it, but I'll dig into the actual security." (P18, Expert)*

Context and User-related Factors

Participants were worried that health data might be used against them in different contexts, including insurance companies, pharmaceutical industries and discrimination of potential employers due to health issues: *"Insurance companies could use the data against me as in the US, but also banks or other organisations." (P1, Expert)*

In the group discussions, it was emphasised that the acceptability of this platform also depended on how severe one's health issues are, mentioning for example HIV and its stigmatisation in society: *"There are many diseases that some people would want to keep to themselves. Especially in the case of HIV patients." (P23, Student)*

4.3. Smart Thermostat Scenario

Figure 5: Most used arguments in favour of and against acceptability of the scenario "smart thermostat"

Perceived Usefulness

A considerable number of participants mentioned energy and financial savings as advantages of this scenario (Figure 5). This is in line with previous research (Paetz et al., 2011) stating that monetary benefits were a crucial driver for adoption of electricity demand regulating smart home devices. Some participants did not see any disadvantages to the scenario: *"To me this is acceptable, it absolutely doesn't disturb me, on the contrary [...]. It is not intrusive to me." (P9, General Population)*

The groups also reflected upon which amount of money would justify the trade-off of having movement data shared, yet there was no consensus on the price value of the savings: *"I would probably use it, if it helps me save a lot of money on my electricity bill. But if it is 10€ a month, not really." (P6, Student)* In another focus group, one participant underlined that even small amounts of money are important. *"That's 120€ a year, that's not nothing!" (P10, General Population)*

Eventually, a considerable number of participants questioned the motives for sharing the data: *"Why does there have to be data sharing? If I have a system here, it can be local. Why do I need to share this - with whom? It does not say it here." (P16, General Population).*

"Energy consumption is not negotiable: it should not be a return for a favor." (P2, Expert)

Perceived Control

Some indicated that tech companies might combine data from different sources and make predictions. The trustworthiness of the company was sometimes questioned.

"I feel like this is almost voyeurism. Sharing data on the rooms in which someone is present, this is extremely personal. And when we see that Facebook can predict a divorce 2 years in advance and that it knows more than the national institute of statistics, we quickly imagine the statistics and predictions made possible by tracking people's presence in the rooms of their house." (P17, Expert)

"The company should be prevented to pair this data with any other data." (P24, Student)

"I don't agree with the fact that I don't know who has access to my data, or for what purpose they will be used, if they will be sold etc." (P15, General Population)

On another negative side, a large number of participants mentioned security concerns, some also considering the potential scaling of burglaries: *"Imagine if you hack an entire district and you know the right moment for break-ins in the entire district." (P32, General Population)*

Context

Overall, participants often stated that more information on the kind of data being collected would need to be specified. Acceptability of the device would therefore depend on how "private" or "sensitive" the type of data shared was perceived by the participants: *"If it is in any way identifying or giving out any information, personal or non-personal data about any of my rhythms or things I do in my house then I would not want to do it." (P3, Expert)*

4.4. Free Social Media Scenario

Figure 6: Most used arguments in favour of and against acceptability of the scenario "free social media".

Perceived Usefulness and Enjoyment

On the positive side (Figure 6), our participants emphasized the enjoyable aspects of social media which make it easy to stay in touch with peers. Other positive remarks referred to the free use of the platform.

More surprisingly, many participants also underlined the advantages of targeted ads, even though this seems hard to admit for some people and led to interesting discussions on profiling. Reacting to a previous comment on the interest of targeted ads, one of the expert participants stated: *"This is something I also wanted to add but then I thought no, I don't want to write this down. But there are some ads I actually like. And there are very often some ads that are so well targeted that I am very happy to discover them. I usually say "Oh come on, that's just another ad…" and then I think "They know me well!"" (P1, Expert)*

The multiplication of accounts was an important negative aspect related to the introduction of "just another social network".

Perceived Autonomy

Several participants appreciated that one was not obliged to use the platform.

On the negative side (Figure 6), a large number of participants indicated that they found too many ads intrusive and annoying. However, they also thought that it is the responsibility of the user to not share sensitive data and to not click on unwanted ads, as stated for instance by this participant: *"Whoever is using it has to be extremely careful in the information they are posting online. At the moment you post it online, it's online forever." (P23, Student).*

Some participants also used this argument to make the point that people who did not like their data being shared were free not to use the platform. *"I am not a dangerous person, I don't write anything about bombing, or drugs and stuff. So for me it is ok, I am fine that WhatsApp will share my data if they need. But for some people (...) they feel unprotected. But then they don't have to use it." (P6, Student)*

Perceived Control

Some participants did not appreciate the lack of control of the data they shared on social media. Many participants also reported feeling "*observed, followed*" *(P9, General Population)*, and mentioned that such a platform should not be advertised as being free, because users "pay" with their data: *"Can we fight against the language of "FREE social media" or "FREE service"? Because simply put, it is not free. We are a file of data, used for statistics, products and so on." (P24, General Population)*

Impact of past experiences

Many also found it acceptable because they already use similar social networks: *"For me this scenario is acceptable because it is the same configuration as Facebook, which I use regularly." (P28, General Population) - "I thought the same thing, given that I use Facebook I cannot say that this type of social platform is not acceptable." (P27, General Population).*

Participants also considered spam one risk of signing up to the social network, but this was not enough to make the scenario unacceptable, given that they were already used to spam. *"The downside is that it will be spam on your email of course, but come on, we have so much already, and I think it is ok." (P6, Student)*

Context and User-related factors

A few participants however distinguished the difficulties of "vulnerable" users who might not be able to differentiate ads from other types of content. *"My sister has a mental disability, when she sees ads I don't think she reacts like me. She would not be really aware that it is an ad." (P15, General Population)*

Participants felt that they were not important enough to be targeted on social media. *"But come on, I am not a famous or popular person, so I don't have this fear that this data will really be used against me." (P6, Student)*

5. DISCUSSION

Our content analysis shows that both acceptance factors and UX factors played a role for participants. Perceived usefulness and ease of use are used in all acceptance models (with similar factors in UX models), while perceived enjoyment, perceived autonomy and the influence of past experiences are linked to hedonic aspects of UX.

5.1. Perceived Usefulness, Ease of Use and Perceived Enjoyment

Across all technology acceptance models, Davis' (1985) dimensions of perceived usefulness and perceived ease of use (or related notions such as performance expectancy and effort expectancy in the UTAUT model (Venkatesh et al., 2003) (Venkatesh et al., 2003, 2012) were considered as major factors explaining behavioral intention to use a system. These factors are comparable to pragmatic qualities of experience in UX models. In the present study, these aspects were indeed discussed extensively across scenarios and seemed to have a strong impact on participants' intention to use or accept the systems. While most participants could clearly see the added value of the health records (improved efficiency of the current scheduling system), the thermostat's usefulness was questioned with regards to the amount of energy saved and the necessity of sharing data. The social network's usefulness was also frequently challenged due to the fact that it did not seem substantially advantageous compared to existing platforms. Similarly, the surveillance cameras were not perceived as useful, and related shortcomings did not outweigh the disadvantages.

Interestingly, when the perceived usefulness of a system was not immediately clear to participants (e.g., the smart thermostat would actually not require any network connection to achieve its mission), one could sometimes note a feeling of mistrust, participants feeling like the company could have a hidden agenda: an apparently innovative technology could be a pretext for getting their data.

Perceived ease of use, on the other hand, was hardly discussed by our participants. Apart from rare mentions to the fact that some technologies could exclude part of the population (mainly the elderly), usability has not been used as an argument in favor or against the acceptability of a scenario. We hypothesize that the nature of the scenarios – rather vague and with no reference to interaction design - made it difficult for participants to imagine perceived ease of use either as a barrier or a facilitator.

5.2. Perceived Enjoyment

Our participants rarely mentioned enjoyment as a relevant factor. The acceptability of the health data scenario for instance was explained with pragmatic aspects (similar to Rainie and Duggan., 2015) and pleasure was not mentioned as a relevant advantage of using an online health platform, which is in line with research by Tavares and Oliveira (2016) who found out that patients do not perceive the use of electronic health record portals as enjoyable. Performance expectancy and effort expectancy (which is comparable to the benefits identified by our participants) on the other hand had a significant impact on

the adoption of online health record platforms. While the smart thermostat has been described by some participants as "innovative", one could not observe a role for perceived enjoyment in that scenario either. In line with Krasnova et al., (2012), performance aspects (saving money / energy) again took the lead here. The closest "hedonic" dimension in the discussions was linked to individuals' values of preserving energy in order to promote a more sustainable way of consuming energy. The fact that perceived enjoyment was rarely mentioned as a relevant factor might also relate to the fact that hedonic factors, while crucial for choice, are only rarely acknowledged at an overt, rational level. This phenomenon is particularly strong when there is a need for justification and an explicit trade-off between hedonic and pragmatic (Diefenbach & Hassenzahl, 2011).

5.3. Perceived Autonomy and Perceived Control

Hedonic UX factors linked to perceived autonomy and control were addressed in all focus groups. The importance of having a free choice of using a technology was highlighted across all scenarios. A frequent argument was also the fact that, if people did not want their data to be sold or used for other purposes, they are not obliged to use a technology. The lack of choice in the office camera scenario, as well as the uncertainty related to what data is collected and by whom it might be watched or used, was often mentioned as a barrier to acceptability.

The need for autonomy can be linked to voluntariness of use, which is one of the moderators of technology acceptance in the UTAUT model (Venkatesh et al., 2003). Beyond voluntariness, perceived control over the information that might be shared to third-parties seems to be one of the main UX factors impacting acceptability. This does not come as a surprise, given that control is a crucial factor in UX needs theories (e.g., (Hassenzahl et al., 2010; Sheldon et al., 2001)), which are considered relevant to technology acceptance (Hornbæk & Hertzum, 2017). A recurring position in all focus groups was for instance that people are keeping the control over what they decide to share on social media. Students and experts mostly felt in control over the information they post, therefore explaining their high level of acceptability. When participants expressed that they perceived the level of control as low, it was mostly linked to low acceptability: *"I don't agree with the fact that I don't know who has access to my data, or for what purpose they will be used, if they will be sold etc." (P15, General Population, in the context of the smart thermostat scenario)*

5.4. Perceived Risks vs. Benefits: a Complex Balance

As mentioned in the literature review, models of privacy calculus take into account perceived privacy risk and privacy concerns (Dienlin & Metzger, 2016; Dinev & Hart, 2006) and suggest that people's intention to disclose personal information depends on a privacy calculus, in which competing factors are assessed and users try to maximize the positive and minimize the negative consequences (Wottrich et al., 2018).

In the present study, the perceived privacy risk was dependent on the scenario. While in the health data scenario the risk of a privacy breach was frequently cited as a concern, in the social media example, the majority of our participants did not really fear that someone might use their data against them. Interestingly, mostly participants in the expert groups mentioned the risk that companies might combine data of different services and make predictions on that basis. This might indicate a low awareness of these practices within "layman" users, and therefore a lower perceived privacy risk impacting their intentions to use specific systems.

It is noteworthy that surveillance cameras were mostly assessed as acceptable by students. As they are not directly concerned by this scenario, one might assume that the perceived risks or disadvantages are low and distant. On the contrary, the very low acceptability ratings of other participants for this scenario might be explained by the fact that the risk of theft is rather small and hypothetical as compared to the immediate and consequent disadvantages employees would experience. It is therefore the perceived benefit that is assessed as too low to be relevant as a trade-off. This is in line with Hallam and Zanella (2017) who found that privacy breaches (in this case security incidents) might seem rather distant and hypothetical, and thus influence behaviour less than short-term consequences.

5.4. The Influence of Previous Experiences

Previous experiences form users' expectations, which then strongly influence users' early evaluations of the usability and enjoyment of a service (Kujala, Mugge, & Miron-Shatz, 2017) and thus play an important role in UX. A relevant observation made during the study refers to the use of personal anecdotes to explain one's opinion, such as the last time a participant went to the doctor and had to wait for a long time, which seemed to strongly influence her acceptance of online health records and their promise of increased efficiency. The same argument was employed in the context of office surveillance cameras, where previous exposure to such practices were used to explain why the participant found the scenario acceptable. Interestingly, these types of reasoning were very frequently used during the discussion phase, but never written down during the individual phase. It seems that past experiences played an important role in participants' acceptability of technology and were used to illustrate and argue during the discussion phase. These past experiences described either critical incidents (e.g., especially

satisfying or dissatisfying experiences in relation to the topic) or ordinary experiences that are integrated as a habit (e.g., cameras when working in a hotel or in a shop). In the first case, it seems like the incidents strongly influenced attitudes and behaviour as a way to cope with the frustration or irritation felt. The second case might be close to the habit factor described by Venkatesh et al. (2012) who state that "the passage of chronological time can result in the formation of differing levels of habit depending on the extent of interaction and familiarity that is developed with a target technology" (p. 161). In addition, the self-consistency bias (Luu & Stocker, 2018) also became apparent in how participants viewed past experiences. Participants exhibited consistent judgements between the past use of a technology (e.g., social media) and why they thought a similar scenario was acceptable: *"given that I use Facebook I cannot say that this type of social platform is not acceptable" (P27, General Population).*

Our findings therefore tend to confirm that feedback from previous experiences indeed influences beliefs and future behavioural performance (Ajzen, 2011; Venkatesh et al., 2003, 2012). Note that these previous experiences are not to be understood necessarily as experiences with technology (acceptance models usually define "experience" as an opportunity to use a target technology (Venkatesh et al., 2012)), given that a negative experience with a "human" service can result in a more positive attitude towards a technology that would increase its efficiency.

At another level, many participants expressed a sort of resignation regarding advertisements, stating that they were so omnipresent that adding another service with ads did not make a real difference. This might point to the phenomenon of privacy fatigue (H. Choi, Park, & Jung, 2018) which refers to exhaustion and cynicism related to managing one's privacy and which has been shown to have a strong influence on privacy-related behaviour.

5.5. The Links Between Technology Acceptance and User Experience in the Context of Privacy Trade-Offs

In summary, our results show that both acceptance factors and UX factors played a role when judging the acceptability of privacy trade-offs. Pragmatic factors such as perceived usefulness were crucial factors for our participants. Hedonic qualities, namely the psychological needs of autonomy and control, also had a strong impact on the perceived acceptability of the scenarios. Our objective of studying non-pragmatic UX aspects that impact acceptance was partly reached. Some hedonic aspects of UX played a role in our study, such as perceived autonomy and control, but the results are non-conclusive with regards to other hedonic aspects. While relying on the scenarios provided by Rainie & Duggan (2015) came with the advantage of using accepted and validated materials on one hand, this material might simply not trigger the necessary emotions to make more far-reaching claims about e.g,. hedonic and enjoyment aspects. We nevertheless believe that these findings are promising and point towards the added value of including users' needs such as autonomy and control in the study of the acceptability of privacy trade-offs. By understanding users' needs, and by supporting their fulfilment through interaction, we can create positive experience and influence users' intention to use a system.

5.6. Individual Judgement vs. Group Discussions

Given that our participants wrote down their perceived advantages and shortcomings of the scenarios individually before the group discussion, we observed that certain aspects were mostly written down, but hardly addressed in the group setting. In the first place, many of the advantages people mentioned individually and which were directly retrievable from the scenarios were not addressed in the groups. This might be due to the fact that these advantages are less controversial and therefore need less discussion, however one might also hypothesize that participants were less convinced of these advantages and mainly wrote them down because they were easily available in the scenario. This phenomenon sheds light on one of the advantages of the focus group methodology. While individually, participants had a tendency to write down the advantages that were easily available, the group discussion phase pushed them to explain further and argue their points of view and to concentrate on the most salient aspects. The social desirability bias might also have influenced participants to focus more on certain aspects, but our homogeneous groups mitigated a part of this bias by helping participants feel at ease expressing their opinions. This also highlights the importance of including both individual and group measures in order to limit this bias.

6. LIMITATIONS

The goal of our study was to go beyond the pragmatic aspects currently covered by most acceptance models to explore the reasons why people accept privacy in certain contexts and build hypotheses regarding additional factors impacting acceptance. We used a qualitative approach, which typically does not have the objective of providing generalizable findings (Leung, 2015) but rather to explore new areas and develop hypotheses (Miles et al., 2014). While we thus do not claim that our results are generalizable, we believe that our analysis speaks beyond the scope of this study. The validity of this research was maximized by sampling a diverse set of participants based on the criteria of nationality, age range and work experience. The coherence of our results with existing theory supports their potential generalizability.

We used a focus group approach in order to provide rich explanations for acceptance of privacy trade-offs. This approach also allowed us to capture diverse viewpoints and observe the reactions of participants who were confronted to privacy concerns that differed from their own. Creating groups of students, experts and groups of the general population has allowed us to understand trends within these groups, which might be explored further in future studies.

Although every effort has been made to ensure the validity of our findings, the present study is subject to limitations that point to opportunities for future research. First, the rationality of privacy-related decisions has been challenged (Acquisti & Grossklags, 2005) and the link between acceptance and actual usage is not clear. A focus group setting that encourages logical explanations might induce a more analytical and rational thinking than might be observed in real-life settings where individuals might not discuss these settings prior to their behaviour. However, this limitation was taken into account in the study design. While focus group discussions cannot predict behaviour in an absolutely accurate way, they did indeed provide us with important insights into factors impacting privacy behaviour. One might point to novel approaches to collecting privacy-relevant data, such as text mining methods using real online customer reviews (Rese, Schreiber, & Baier, 2014), which might be relevant when exploring privacy trade-offs as they actually study acceptance of systems in use and not only the projection of acceptability. Their limitation however is that people usually report particularly satisfying or dissatisfying experiences, also called critical incidents.

From a methodological perspective, we are aware that certain arguments occur frequently because they were obvious from the scenario descriptions. We have highlighted these apparent arguments in the results section and have discussed the salience of arguments by comparing those who were produced individually versus during the discussion.

Our sample composition also presents inherent limitations, as a qualitative approach using focus groups usually does not reach a sample representative of the entire population. While the inclusion of contrasting groups (experts, students, general population) is already an asset of the present study, we did for instance not include teenagers or retired persons in our sample. This might be relevant for future work as some demographics have been shown to influence privacy-decisions (Rainie & Duggan, 2015). Cultural differences might also play an important role in privacy. Despite the fact that we had a diverse set of participants in terms of nationalities represented, the sample for each nationality was too small to derive any conclusions; we did not control for cultural bias.

For the online focus groups, we used Facebook as a platform, which excluded those who did not have a Facebook account or did not want to participate in a discussion group on this social network. This limitation was partially mitigated through the use of face-to-face focus groups.

7. Future Work and Recommendations For Updated Technology Acceptance Models in the Context of Privacy Trade-offs

Taking into account these limitations, and building on the promising findings, we are planning for future work to include a quantitative questionnaire. It will allow us to exploit the results of this qualitative study and reach a more representative sample of the population over a number of different channels to exclude biases linked to the use of one social network only. The questionnaire will also take into account UX needs so as to further verify ties with UX, and the privacy paradox with the goal of evaluating not only the acceptability of the scenarios, but also the alignment of this acceptability with real-life actions. We also believe that future studies should conduct a more in-depth research on the influence of the human needs (Hassenzahl et al., 2010; Hornbæk & Hertzum, 2017; Sheldon et al., 2001) as these theoretical models and related design tools might be a great support for designers trying to cope with users' privacy concerns. In a health context, Angst and Agarwal (2009) have for instance shown that even potential users with high levels of privacy concern can change their attitudes positively if message framing is adapted accordingly.

In order to support the inclusion of these theoretical models into practice, we recommend that design teams should strive to understand users' **needs** in the context of privacy trade-offs. Supporting fulfilment of these needs through the interaction might well influence users' privacy trade-offs and intention to use a system. Our results show that the needs of **autonomy and control** have an important influence on the acceptability of privacy-relevant technologies as participants wanted to be free to choose whether they wanted to use a technology, and they felt uneasy with the loss of control of their data. When creating an integrated model that bridges UX and TA research for application in the context of privacy-related technologies, the impact of these concepts should be closely investigated in detail. While in our study, autonomy and control were prevalent, design teams should also use existing tools to explore other needs that are relevant for their experience (e.g., UX Needs Cards (Lallemand, 2015)).

Another relevant UX factor when designing privacy-relevant experiences is the influence of **past experiences.** One should thus explore which past experiences users compare one's product or service to. Benchmarking such comparable experiences can help understand users' mental models and design their experience accordingly. In addition, closer examination of the self-consistency bias in the context of privacy trade-offs seems worthwhile.

Our study also shows that the acceptance of privacy trade-offs is highly **context-**dependent. We recommend that design teams studying acceptance should explore context-related factors in the design process, for example using tools such as contextual inquiry (Holtzblatt & Beyer, 2016) and synthesizing through user journey maps (Kalbach, 2016).

7. CONCLUSION

In the present study, we conducted focus groups with 32 participants in order to understand factors influencing their privacy trade-offs in four different use scenarios and to match these factors to both acceptance and UX frameworks. Our contribution consists in the rich qualitative insights elucidating the factors that influence the extent to which users accept privacy trade-offs, pointing to a selection of ties between acceptance and UX factors. While this calls for further research, it also points out that pragmatic aspects alone are insufficient for explaining privacy trade-offs; a prominent example is that of "control" or "autonomy" suggesting that factors outside the conceptual space of technology acceptance dimensions are just as relevant. This further illustrates how human behaviour is likely to depend not only on security and privacy awareness and that designers need to consider the technology and experience design as a whole instead of focusing on single aspects.

At a larger level, we expect the results of this study to contribute to the development of user-centred privacy initiatives and to the enrichment of current theoretical models of technology acceptance with additional aspects drawn from the field of UX.

8. ACKNOWLEDGEMENTS

(Anonymized)

9. REFERENCES

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Al-Sharafi, M. A., Arsha, R. A., Abu-Shanab, E., & Elayah, N. (2016). The Effect of Security and Privacy Perceptions on Customers' Trust to Accept Internet Banking Services: An Extension of TAM. *Journal of Engineering and Applied Sciences 11(3):545-552*, 9.

Angst, C. M., & Agarwal, R. (2009). Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion. *MIS Quarterly*, *33*(2), 339–370. https://doi.org/10.2307/20650295

Blandford, A., Furniss, D., & Makri, S. (2016). Qualitative HCI research: Going behind the scenes. *Synthesis Lectures on Human-Centered Informatics*, *9*(1), 1–115.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Choi, B. C. F., & Land, L. (2016). The effects of general privacy concerns and transactional privacy concerns on Facebook apps usage. *Information & Management*, *53*(7), 868–877. https://doi.org/10.1016/j.im.2016.02.003

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (PhD Thesis). Massachusetts Institute of Technology.

Desmet, P., & Hekkert, P. (2007). Framework of Product Experience. *International Journal of Design*, *1*(1).

Diefenbach, S., & Hassenzahl, M. (2011). The dilemma of the hedonic – Appreciated, but hard to justify. *Interacting with Computers*, *23*(5), 461–472. https://doi.org/10.1016/j.intcom.2011.07.002

Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, *21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Distler, V., Zollinger, M.-L., Lallemand, C., Roenne, P. B., Ryan, P. Y. A., & Koenig, V. (2019). Security—Visible, Yet Unseen? *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–13. Glasgow, Scotland Uk: ACM.

Egea, J. M. O., & González, M. V. R. (2011). Explaining physicians' acceptance of EHCR systems: An extension of TAM with trust and risk factors. *Computers in Human Behavior*, *27*(1), 319–332. https://doi.org/10.1016/j.chb.2010.08.010

Hallam, C., & Zanella, G. (2017). Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, *68*, 217–227. https://doi.org/10.1016/j.chb.2016.11.033

Hassenzahl, M. (2008). User experience (UX): Towards an experiential perspective on product quality. *Proceedings of the 20th Conference on l'Interaction Homme-Machine*, 11–15. ACM.

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. *Interacting with Computers*, *22*(5), 353–362. https://doi.org/10.1016/j.intcom.2010.04.002

Hassenzahl, M., Eckoldt, K., Diefenbach, S., Laschke, M., Len, E., & Kim, J. (2013). Designing moments of meaning and pleasure. Experience design and happiness. *International Journal of Design*, *7*(3).

Hassenzahl, M., & Tractinsky, N. (2006). User experience—A research agenda. *Behaviour & Information Technology*, *25*(2), 91–97. https://doi.org/10.1080/01449290500330331

Holtzblatt, K., & Beyer, H. (2016). *Contextual design: Design for life*. Morgan Kaufmann.

Hornbæk, K., & Hertzum, M. (2017). Technology Acceptance and User Experience: A Review of the Experiential

Component in HCI. *ACM Transactions on Computer-Human Interaction*, *24*(5), 1–30. https://doi.org/10.1145/3127358

Kalbach, J. (2016). *Mapping experiences: A complete guide to creating value through journeys, blueprints, and diagrams*. O'Reilly Media, Inc.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture: Intercultural Dynamics of Privacy Calculus. *Business & Information Systems Engineering*, *4*(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Kraus, L., Wechsung, I., & Möller, S. (2016). *Exploring Psychological Need Fulfillment for Security and Privacy Actions on Smartphones*. https://doi.org/10.14722/eurousec.2016.23009

Kraus, L., Wechsung, I., & Möller, S. (2017). Psychological needs as motivators for security and privacy actions on smartphones. *Journal of Information Security and Applications*, *34*, 34–45. https://doi.org/10.1016/j.jisa.2016.10.002

Krueger, R. A., & Casey, M. A. (2014). *Focus Groups: A Practical Guide for Applied Research* (5th Edition). Retrieved from https://books.google.fr/books?id=APtDBAAAQBAJ

Kujala, S., Mugge, R., & Miron-Shatz, T. (2017). The role of expectations in service evaluation: A longitudinal study of a proximity mobile payment service. *International Journal of Human-Computer Studies*, *98*, 51–61. https://doi.org/10.1016/j.ijhcs.2016.09.011

Lallemand, C. (2015). *Towards consolidated methods for the design and evaluation of user experience*. University of Luxembourg, Luxembourg.

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324–327. https://doi.org/10.4103/2249-4863.161306

Luo, X., Li, H., Zhang, J., & Shim, J. P. (2010). Examining multi-dimensional trust and multi-faceted risk in initial acceptance of emerging technologies: An empirical study of mobile banking services. *Decision Support Systems*, *49*(2), 222–234. https://doi.org/10.1016/j.dss.2010.02.008

Luu, L., & Stocker, A. A. (2018). Post-decision biases reveal a self-consistency principle in perceptual inference. *ELife*, *7*, e33334. https://doi.org/10.7554/eLife.33334

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative Data Analysis*. Retrieved from https://books.google.lu/books?id=3CNrUbTu6CsC

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Osswald, S., Wurhofer, D., Trösterer, S., Beck, E., & Tscheligi, M. (2012). Predicting information technology usage in the car: Towards a car technology acceptance model. *Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*, 51–58. Portsmouth, New Hampshire: ACM.

Paetz, A.-G., Becker, B., Fichtner, W., & Schmeck, H. (2011). Shifting Electricity Demand with Smart Home Technologies—An Experimental Study on User Acceptance. *30th USAEE/IAEE North American Conference Online Proceedings, Washington DC, 9-12 October 2011.*, 19.

Rainie, L., & Duggan, M. (2015). *Privacy and Information Sharing*. Pew Research Center.

Rese, A., Schreiber, S., & Baier, D. (2014). Technology acceptance modeling of augmented reality at the point of sale: Can surveys be replaced by an analysis of online reviews? *Journal of Retailing and Consumer Services*, *21*(5), 869–876. https://doi.org/10.1016/j.jretconser.2014.02.011

Schade, J., & Schlag, B. (Eds.). (2003). *Acceptability of Transport Pricing Strategies: An Introduction*. Retrieved from https://www.emeraldinsight.com/doi/pdfplus/10.1108/9781786359506-001

Shackel, B., & Richardson, S. J. (1991). *Human factors for informatics usability*. Cambridge university press.

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. *Journal of Personality and Social Psychology*, *80*(2), 325.

Tavares, J., & Oliveira, T. (2016). Electronic Health Record Patient Portal Adoption by Health Care Consumers: An Acceptance Model and Survey. *Journal of Medical Internet Research*, *18*(3), e49. https://doi.org/10.2196/jmir.5069

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Venkatesh, V., & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a

Unified View. *MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. *MIS Quarterly 36(1):157-178*, 22.

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

Wottrich, V. M., van Reijmersdal, E. A., & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Wu, I.-L., & Chen, J.-L. (2005). An extension of Trust and TAM model with TPB in the initial adoption of on-line tax: An empirical study. *International Journal of Human-Computer Studies*, *62*(6), 784–808. https://doi.org/10.1016/j.ijhcs.2005.03.003

Highlights

- Applicability of technology acceptance models to privacy and security contexts
- Hedonic factors should be included in acceptance models to assess privacy trade-offs
- Perceived usefulness, previous experiences, autonomy and feeling of control over data
- Implications for the design of privacy-relevant systems