Quality and User Experience (2025) 10:4
https://doi.org/10.1007/s41233-025-00074-5

ORIGINAL PAPER

Exploring users' privacy decision making in retail– insights and challenges for HCI research

Emilie Storslett Henriksen[1] · Asbjørn Følstad[2] · Konstantinos Boletsis[2]

Received: 16 August 2024 / Accepted: 21 June 2025

Abstract
Privacy is an area of substantial societal debate and research interest. Increased sharing and processing of personal data enables personalized systems and services, but also entails substantial costs in terms of surveillance and loss of privacy. Retail is a domain where tensions of costs and benefits concerning data sharing is particularly evident and, hence, a domain of high potential interest to HCI research on privacy. We have conducted an exploration of user' decision-making process when sharing personal data in retail, through semi-structured interviews with 14 participants. The interviews shed light on data sharing habits– identifying convenience-oriented, opportunistic, or risk-oriented approaches– as well as the relevance of privacy calculus and factors skewing their privacy decisions. Participants typically were able to explicate their calculations prior to data sharing, considering relevant negative and positive consequences. At the same time participants also acknowledged cognitive, emotional, social, and contextual factors that could skew their privacy calculus. Key findings from the interviews were validated in a follow-up questionnaire study with 191 participants. Through reflection on the findings relative to the existing body of knowledge, we propose three key future challenges for HCI research on retail, to help users scope, balance, and act on their privacy considerations.

Keywords User research · Data sharing · Decision making · Privacy · Retail

Introduction

Privacy concerns are inherent in interaction with service providers and interactive systems [10]. Any user of digital technology– indeed, any member of modern society– are likely to have their personal data processed in myriad computer systems. From a user perspective, allowing applications, websites, and service providers in general to process personal data can be beneficial, given that such processing is required to achieve users' specific goals or objectives [4]. Sharing personal data allows access to personal services or content as well as personalization of general information or services [3]. In brief, sharing personal data is currently interwoven in key functions of society.

At the same time, privacy concerns represent a source of substantial uncertainty and discomfort for users [46]. In part, such discomfort is related to fear of privacy breaches where unauthorized actors gain access to personal data with potential implications for misuse [45]. In part, it concerns the notion of surveillance capitalism [76] where monetizing user data is increasingly important to service providers. Here, sharing personal data allows service providers to make use of these data for purposes not requested or even desired by users, such as customer segmentation, promotional campaigns, and targeted advertising [72]. Under this perspective, while users may seem to benefit from data sharing in that they get access to information and services for free, the costs may ultimately threaten individuality, free will, and liberal society [77]. In consequence, privacy concerns have generated substantial public engagement and motivated legislation, such as the European GDPR [25].

Privacy concerns have been a longstanding object of research and discussions within the Human-Computer Interaction (HCI) community. Privacy by design have been discussed for ubiquitous computing since the turn of the century [1, 40], numerous user studies have addressed privacy perceptions and behaviours [35], substantial work has been done on privacy and design [22, 50], and personal data

✉ Asbjørn Følstad
asf@sintef.no

[1] Kristiania University of Applied Sciences, Oslo, Norway

[2] SINTEF, Oslo, Norway

Published online: 12 July 2025

processing has been debated in the context of vulnerable groups [49].

Still, despite HCI research and discussion, as well as public debate and legislation, it is hardly an overstatement to claim that consumer contexts still entail important privacy challenges. Due to increasing computerization of public and private spaces, sharing of personal data not only concerns online service provision but also activities in the physical world such as transportation, social events, and shopping [34].

The retail context is particularly illustrative of current privacy challenges [61]. Retail is a driver of targeted advertising, tightly associated with surveillance capitalism [74]. Furthermore, processing of personal data is increasingly taking place in both online and offline shopping contexts through a blending of digital and physical provision of information and services [10]. At the same time, the retail context illustrates the potential benefits in the sharing of personal data, as this unlocks utility-oriented and experiential benefits [56].

As such, the retail context is an interesting point of departure for discussions of privacy challenges within HCI. Through a user-centred perspective, HCI research should be able to identify and develop solutions enabling substantiated needs for sharing and processing of personal data while mitigating confusing and uncomfortable user experiences associated with surveillance capitalism. As basis for this discussion, we in this paper present a qualitative interview study of user perceptions of data sharing in retail and their decision processes for such sharing. Based on this study, and a quantitative follow-up to validate its key findings, we discuss privacy experiences in retail, and– more generally– how this insight can motivate a discussion of the objectives for privacy research in HCI.

Through this study, we contribute insights that may motivate renewed reflection and discussion of privacy challenges in HCI and how to address these from a user-centred perspective. Specifically, we propose the need for solutions that enable users to scope and balance their privacy considerations, as well as bringing these considerations to bear on users' actions.

Background

Privacy concerns in retail

Consumer retail is a domain where privacy issues are acutely palpable [51]. Retailers seek to attract users, strengthen user relations, and personalize the service journey, through capture and use of what Martin and Palmatier [46] refer to as "vastly increased personal information". For users of retail services, their personal data are sought when browsing and searching for products online, when visiting stores, conducting payments, or having products brought home, as well as post-purchase returns, complaints, recommendations, or repurchase [11]. The increase in personal data capture and use in physical retail has strengthened privacy concerns [52]. In response, a substantial body of research on privacy in retail has evolved. A review by Marriott and colleagues [43] identified more than 130 relevant studies.

Privacy concerns are highly relevant for online retail interactions, with data capture throughout the digital service journey [61]. Such concerns are also increasingly relevant for in-store retail interactions due to the uptake of digital support for retail, e.g. in the form of retail apps, customer clubs, and payment and credit solutions as part of so-called omnichannel retail [56]. Just about any user interaction with a retailer entails an opportunity or request for sharing personal data, and the online and in-store modes of retail increasingly blur due to a turn towards omnichannel approaches where online and in-store customer interactions blend and data flows between the online and in-store context [10]. When sharing personal data, users may be limited in their capacity or interest in considering how these are used by the retailer or in the network of service providers supporting the retailer service processes, though privacy concerns are on the rise [30]. Furthermore, users may have insufficient insight into the consequences of data sharing, be it potentially negative implications– such as undesirable marketing activity– or potential benefits, such as an improved user experience or reduced cost [57].

In response to the importance of personal data for service personalization and broad presence of privacy issues in service provision, along with increasingly strong privacy regulation [25], privacy is a stated priority of retailers as well as users. In a recent Cisco privacy benchmark report [14], >90% of companies reported that customer patronage depends on data being properly protected. In a consumer report by the same firm [13], 33% of surveyed users reported to be privacy active.

At the same time, concern is voiced with regard to insufficient research attention to privacy in retail. Martin and Palmatier [46], in their introduction to a special issue on data privacy in retail, noted the tension between users' desire for personalization and privacy as a reason for this being an area of continued challenge– though a common interest in retailers, regulators, and users to preserve privacy. Furthermore, they noted tensions in how user approaches to privacy are construed by researchers as either (a) a privacy paradox or (b) a consequence of users not being sufficiently aware and knowledgeable to protect themselves from potential harms of personal data sharing. In response to these issues, they argue that "the extent to which customers are actually

knowledgeable about the implications of their interactions with retailers is an open question" [46] and call for research addressing users' actual knowledge of privacy and privacy implications in retail.

Privacy research in HCI

HCI research on privacy is fundamentally about empowering users to make informed and confident decisions regarding their personal information [31, 37, 61]. Privacy decision making is particularly important in a world dominated by digital interactions and data exchanges. This research often focuses on the development and evaluation of interfaces that help users understand and manage their privacy settings more effectively.

One prominent approach within HCI for supporting privacy decisions is the design of user interfaces that clearly communicate privacy implications of various choices. To support users in understanding and controlling their privacy settings, researchers have explored the design of privacy notices. This involves creating user-friendly visualization metaphors that users can understand easily, thereby aiding them in making informed decisions about their privacy [37]. In this context, "privacy facts" [38], i.e., labels with privacy-related information, and "privacy icons" [20, 31] have been suggested as means to help users understand the privacy policies before making a privacy-related decision, e.g., accepting the privacy statements of mobile applications or websites.

Similarly, conceptual models and frameworks have been suggested to guide privacy-by-design processes and integrate privacy-awareness elements during the initial stages of the design process. Feng and colleagues [22] contributed a conceptual framework that considers privacy choice as a user-centred process that guides the development of privacy user interfaces. At the same time, conceptual work to support user privacy awareness has been conducted for specific technologies. For example, HCI research in cloud data protection tools has sought to enhance transparency and accountability in user interface design, thus supporting informed user decisions [24]. Leschanowsky and colleagues [41] focused on designing privacy strategies for Conversational AI systems, investigating how different strategies affect users' perceptions and their alignment with desired privacy outcomes. Finally, Prillard and colleagues [55] examined user privacy awareness and transparency in the Metaverse, proposing a set of suggestions for ethical privacy design for this context. This type of research is crucial for developing systems that not only respect user privacy but also evoke trust and confidence.

In addition to interface improvements, there is also emphasis on incorporating user preferences and behaviours into privacy controls. Wijesekera and colleagues [68] conducted extensive field studies to tailor privacy settings in Android systems to match users' actual preferences, significantly reducing errors in privacy settings while maintaining usability. This aligns with ongoing efforts in HCI to develop predictive models that understand and anticipate users' privacy preferences based on their past behaviour, such as the work by Tøndel and colleagues [66] on learning privacy preferences through machine learning techniques.

Privacy decision support systems also integrate contextual factors that affect user decisions. Schaub and colleagues [59] proposed a context-aware privacy framework that adapts to changes in user's environments, enabling dynamic privacy decisions that reflect the current context. This reflects a broader trend in HCI to utilize context as a crucial factor in privacy management.

Related to research on how to design for supporting users' privacy decision making, significant work has also been done on the identification and mitigation of user interface design that obstruct or bias users' privacy decisions. Important in this regard is concept of dark patterns, that is, manipulative designs that "influence users to purchase goods and subscriptions, spend more time on-site, or mindlessly accept the harvesting of their personal data" [7]. This could, for example, concern cookie consent banners at websites that may be designed in ways perceived as unacceptable or unfair [8]. Gray and colleagues [29] listed and discussed common dark patterns in user experience (UX) design, including patterns for privacy, and detailed common dark pattern strategies such as nagging, obstruction and forced action to manipulate users into favourable outcomes for the service owner provider at the cost of the user. On basis of a user study, Gray and colleagues [28], suggested that the manipulation felt by users when confronted with dark patterns could indicate that user awareness is a first step towards mitigation of manipulative design practices.

By improving the design of privacy interfaces, integrating adaptive privacy controls, and enhancing transparency, as well as exposing and helping to mitigate manipulative practices, HCI can significantly contribute to better privacy management in digital environments. These research efforts provide foundational insights for developers and policymakers to build more trustworthy and user-friendly systems.

Decision making for personal data sharing

Service providers are required to gather users' informed consent prior to sharing of personal data, by means of increasingly thorough regulation [53], users' sharing of personal data in retail can be conceived of as a decision-making process. Clearly, this process can be more or less thorough depending on the priorities and circumstances

of the individual user, but provided personal data is not captured without due notice there is a decision process involved. In the following, we will review three approaches to understanding this decision-making process: privacy calculus, decision making in practice, and a potential privacy paradox.

Privacy calculus

'Privacy calculus' refers to the rational calculation of drivers and inhibitors associated with personal data sharing. Drivers may include personal benefits, perceived control, and trust. Inhibitors may include perceived cost, risk, and privacy concerns [16]. The privacy calculus, hence, involves users' rudimentary analyses of potential risks and benefits prior to sharing of sharing of personal data [15], which in turn may guide their behaviour [12, 62].

Privacy benefits concern potential rewards or gains the user may get in return for personal data sharing, such as personalization or monetary incentives. Privacy risk concerns the perceived potential negative implications of personal data sharing, which may negatively impact user's privacy concerns [62].

Drawing on previous literature, Beke and colleagues [6] found that privacy calculus could entail assessments of risks and benefits concerning a range of aspects, including the expected service performance and security levels, outcome expectations, service provision time, and psychological, emotional, or social aspects. Marwick and Hargittai [47], in a qualitative user study, found that users were particularly aware of distinctions between different information types, contexts, and recipients of information when making privacy decisions.

The notion of privacy calculus has been the subject of substantial research across several decades, and substantial empirical evidence suggests the relevance of rational assessments of risks and benefits for users' data-sharing decisions, though the real-world manifestations of privacy calculus may not be as straight forward as survey-based or experimental studies suggest [15].

Privacy decision making in practice

While the privacy calculus perspective assumes data sharing following a rational calculation of benefits and risks, rationality may not entail a sufficiently comprehensive explanation of data sharing behaviour.

Fernandes and Pereira [23] argued for the need to revisit the assumptions of privacy calculus, as they found that risk-benefit assessments of data sharing are not fully rational. In a questionnaire study, they found evidence of this as users' utilitarian benefits and hedonic motives may outweigh privacy concerns, suggesting that while privacy calculus may indeed be relevant in a decision process, the calculus may be skewed by elements of user irrationality.

In part, such irrationality may be explained by limited cognitive processing capacity, where reflection on the beneficial use of a specific service may be given priority over reflection on privacy concerns, as demonstrated in an experimental study by Fu and colleagues [26]. Furthermore, in a review of the literature on privacy and security in decision making, Acquisti and colleagues [2] noted that users, when making decision to share personal data, are limited by incomplete information available which in turn requires reliance on heuristics for decision making.

Users' privacy calculations may further be impacted by other factors, such as trust, emotion, and social factors. Dinev and colleagues [16] in a study of data sharing in online retail demonstrated the impact of users' propensity to trust and institutional trust when making decisions with privacy implications. Zhang and colleagues [75], in an interview study of media technology users, found people to be impacted by folk theories, cognitive aspects and emotion in their privacy decisions. Kehr and colleagues [36] in an experiment on data sharing in a smartphone application context, found that privacy assessment may be impacted by momentary emotional states, e.g., due to positive affect resulting from an interactive service. Trepte and colleagues [67]., in an online experiment on personal data sharing, demonstrated that while users to some extent behave as might be expected from the perspective of a privacy calculus– where higher privacy concerns were associated with a reduced willingness to share personal data– such calculations may also be impacted by social influence– demonstrated by the impact of providing information on other users' choices of information sharing.

A privacy paradox?

In consequence of the range of factors which may impact users' decisions to share personal data, users have been found to display a disconnect between their own data sharing habits and their perceptions of these [5, 12], or to display an inconsistency with regards to how they think and behave with regards to data sharing [29]. That is, while users on the one hand claim to be privacy concerned, they on the other hand may be willing to share personal data for relatively small benefits [39] without thorough consideration of privacy implications or mitigation mechanisms [15].

Such seemingly paradoxical behaviour may be exemplified e.g. in users' disregard of their privacy rights when consenting to data sharing. European legislation requires website owners to gather informed consent from users when gathering personal information. Such legislation has

motivated potential means for users to mitigate privacy issues, e.g. by gathering information on data sharing and purposes. While users have been found typically to have knowledge on their privacy rights according to European legislation, few report to be inclined to take advantage of these rights [54].

However, in a systematic review of literature on privacy attitudes and behaviour, Gerber and colleagues [27] found that the literature strongly supports the notion of privacy calculus in users' data sharing decisions, with personal gains from data sharing to be among the strongest drivers of personal data sharing. In consequence of the evidence in support of privacy calculus in users, the privacy paradox has by some been referred to as an unsubstantiated myth [63]. Others, more favourably, have discussed it as a non-paradoxical phenomenon which may be explained by factors associate with the service, the user, or the context that potentially impacting rational privacy decisions [27].

An alternative perspective on the privacy paradox that has emerged in privacy research, is that of privacy resignation, that is, the sense of disempowerment in users in the face of personal data sharing decisions [18]. For a privacy calculus to impact decision making and behaviour, users need to have a sense of control or empowerment with regards to their data sharing practices. Hargittai and Marwick [32], in a qualitative user study, found that even privacy savvy users expressed resignation, apathy and cynicism concerning personal data sharing online– largely due to the desire to interact socially online, networked privacy issues, and what they saw as inevitable privacy breaches. Privacy resignation may be seen as an alternative perspective on practices for sharing personal data as guided mainly by rational decisions over which the individual user has control. As discussed by Draper [17], the challenges due to the networked nature of online interactions and the overwhelming task it is for users to take reasoned action with regard to data sharing, make users feel they have no real choice but to share data– to an extent that even privacy engaged users may lose faith in their ability to keep up with their desired standards for privacy protection.

Privacy segmentation

Concluding this background section, we provide an overview of a previous research on privacy segmentation, that is, whether users can be meaningfully grouped with regard to similarities in privacy perceptions and behaviour. A much cited privacy segmentation framework is Westin's [70] distinction between what he referred to as (a) fundamentalists, characterized by high levels of privacy awareness, scepticism of organization's claims to personal data, and acknowledgement on the need for privacy regulation, (b) pragmatists, characterized by moderate privacy concerns and a willingness to share personal data in exchange for clear benefits, and (c) unconcerned, characterized by limited interest in and concern for privacy decision making, as well as trust in organizations to handle data properly.

This segmentation was established in the mid-nineties, and has since been applied, sought adapted, and criticised. An example of direct application is Watson and colleagues' [69] use of the segments to explore how privacy defaults can be adapted to user preferences. An example of adaptations to the Westin segmentation is provided by Dupree and colleagues [19] who identified five user clusters as part of a design-oriented study, including fundamentalists, lazy experts, technicians, amateurs, and marginally concerned.

There has also been substantial criticism of Westin's privacy segmentation. One strain of criticism has noted that empirical findings suggest limited value of user segments for prediction of privacy behaviours [71]. Advancing this criticism, researchers such as Martin and Nissenbaum [44] and Yang and colleagues [73] have argued for the importance of contextual determinants for users privacy decisions. A second strain of criticism has confronted the notion of rational privacy decision making assumed by Westin and argued for the need to instead protect users without sufficient means to engage in healthy privacy protection practices. For example, researchers such as Hoofnagle and Urban [33] distinguished between privacy resilient and privacy vulnerable users. Particular sensitivity is required by service providers requesting personal data from the latter user group.

Adding to the above, a range of other attempts at distinguishing between user segments or categories have been made. For example, Bughin [10] identified seven market segments of users in terms of their trade-offs between privacy and usage. Egelman and Peer [21] explored psychological factors explaining variation in privacy perceptions and behaviour. There has also been research returning resembling segments to those provided by Westin [48, 60]. For example, Schomakers and colleagues [60] identified a tripartite segmentation of users constituted of privacy guardians, -pragmatists, and -cynics. When we in our study explore user approaches to data sharing, we tie into this backdrop of existing research and knowledge.

Research questions

While there is a large and growing knowledge base on privacy in HCI, there is an acknowledgement that substantial privacy challenges exist in service provision and interactive systems. Retail is a market sector where privacy challenges are particularly evident, as users' digital information is increasingly leveraged by retailers in online as well as

offline contexts. At the same time, retail arguably is a market sector where the potential benefits of personal data sharing are immediately evident to users through rewards and improved service.

Based in existing research, and in our assumption that privacy challenges merits further debate in HCI, we formulated the following research questions for this study.

RQ1. What characterizes users' decision-making process when sharing personal data with retail service providers?

RQ2. Which research challenges are particularly relevant for HCI to help reduce users' privacy concerns?

RQ1 motivated us to review user insight in a specific market domain where privacy challenges– and benefits of data sharing– are concrete and imminent. RQ2 motivated a broader discussion on the basis of the user insight and existing knowledge. Hence, RQ1 will mainly be addressed through the findings in the results section while RQ2 will be addressed through a discussion of these findings.

Method

Research design

The overall research design was set up as an exploratory qualitative interview study, complemented with a questionnaire-based follow-up, in the context of retail. This choice of research design was motivated by a need to gather updated and contextualized information on users' privacy decisions, to enable reflection and discussion on how gathering and processing of personal data in services and interactive systems can be improved. The study was conducted in a Norwegian retail context, which is helpful given the relative high uptake of digital and online services among users in this country. Data from Statistics Norway show that 99% of Norwegians are online, 96% use internet banking, and > 50% us the internet to by items such a clothes [65].

Qualitative data were gathered through semi-structured interviews with 14 participants, conducted as part of a master thesis project in digital business systems. In a subsequent follow-up questionnaire study, data were gathered from 191 participants from the retail context to gain further insight into the broader relevance of the themes identified in the interview study.

Participants and recruitment

To allow for a sufficient span in the participant group in the interview study, recruitment of participants was set up so as to distribute these across users with different attitudes towards adoption of technology. Specifically, we used Rogers' [58] theory of diffusion of innovations, to distinguish broadly between users characterized as earlier adopters and later adopters with regards to innovations in retail, such as their use of online solutions, customer apps, and loyalty programs.

Participants were recruited through a questionnaire distributed in the social media and professional networks of the authors. This recruitment was seen as adequate given the objective of the research to inform exploration. To assess participant attitude towards innovations in retail, questions addressed the participants self-reported inclination to identify and make use of new digital solutions in retail, as well as their perceived influence on others' use of digital solutions in retail through advice or information.

In total, 54 potential participants signed up through the questionnaire. Of these, interviews were conducted with 14 participants, eight male and six female. Of these, eight were characterized as earlier adopters (five male, three female) and six as later adopters (three male, three female). The age of the participants spanned from 20 to 61 years (mean = 31, $SD = 15$). The interviewed participants all received a gift card of approximately 25 Euro value.

In the follow-up questionnaire study, data were gathered from a sample of 191 participants recruited from a Norwegian marketing panel. The participants were recruited to ensure experience with online grocery retail. All participants had at least shopped groceries online once or a few times, and 53% engaged in online shopping of groceries monthly or more. The participants were also recruited so as to do at least half of the grocery shopping in their household, with 86% reporting to do more than half of such shopping. The sample was balanced with regards to gender (49% males, 51% females). Participant age ranged from 30 to 60 years, with 51% in the 30–45 year bracket and 49% in the 46–60 year bracket. The majority of the participants (78%) reported to live in households with two or more residents, and nearly half the participants (43%) reported to have children in the household. The participant sample for the questionnaire study did not overlap that of the interview study.

The participant age brackets in the online follow-up study correspond well with demographic characteristics of frequent users of online grocery retail, with millennials– born in the years between early 1980'ies and mid 1990'ies– leading the charge and the baby boomer generation– born up to the mid 1960'ies lagging behind [64].

Interviews

The interviews were semi-structured to allow for sufficient exploration of participants experiences concerning personal data sharing in retail, as well as their perspectives on the data sharing decision process.

The interview guide was structured in four parts, addressing the following main themes:

- Experiences and perceptions on personal data sharing.
- Habits of data sharing.
- Decisions on data sharing and the decision-making process.
- Knowledge and perceived impact of privacy regulation.

Throughout the interview, the participants were encouraged to reflect on online as well as offline or in-store data sharing. All interviews were conducted through an online meeting solution (Microsoft Teams) for ease of access to participant as well as to gather data from a broader geographical distribution of participants. Mean interview duration was 27 min (range: 19–41 min).

Prior to data collection, the interview guide and procedure were tested and improved through two pilot interviews. The procedure and guide were also assessed and confirmed after four of the main interviews.

Analysis

All interviews were recorded and transcribed. Analysis was conducted in line with Braun and Clarke's [9] recommendations for thematic analysis.

The analysis generated 44 initial codes. These were grouped into higher level subthemes which in turn was grouped into themes concerning habit (sharing / non-sharing), privacy calculus (positive / negative consequences), privacy paradox (implicit / explicit), external factors (contextual, emotional, social), and regulation through GDPR (knowledge, control).

The analysis process was conducted by the first author. To strengthen quality in analysis, meetings for critical review at the different stages in the process for thematic analysis was conducted with the second author. The second author also revisited the analysis to establish exact counts of occurrences for the different themes and assess the prevalence of different approaches to personal data sharing.

In the presentation of the findings from the interview study, the number of participants reflecting on each theme is provided for transparency and to indicate the prevalence of each theme.

Follow-up questionnaire study

The questionnaire study was conducted as a follow-up to gain further insight into the main themes of the interview study. Hence, the questionnaire included questions concerning the main identified themes on approaches to personal data sharing as well as negative and positive consequences of personal data sharing of relevance to privacy calculus. The questionnaire study participants were also asked about their privacy concerns for validation purposes and for insight into this aspect. The questionnaire items are presented in the Appendix.

Based on their responses on approaches to personal data sharing, the participants were divided into three groups reflecting their main identified approaches to personal data sharing. The relative prevalence of the different approaches were assessed, as well as their tendency to covary with six identified themes related to privacy calculus.

Analyses of group differences were conducted by SPSS v29. Group differences were conducted by way of ANOVA and Tukey HSD pairwise comparisons with Bonferroni correction. Due to observed non-normality in distributions, all analyses were replicated with the non-parametric Kruskal-Wallis test. Non-parametric test results largely showed the same pattern as the parametric tests and are not reported for the sake of brevity as these.

Research ethics

Participant involvement and processing of their personal data were only conducted following approval from the relevant data protection body as well as informed consent from participants. All participant data from the interview study was anonymized as part of the analysis process. The follow-up questionnaire study was conducted without the gathering of personal data.

Results

In the results section, we first provide an overview of key finding from the interviews. These concern data sharing habits, privacy calculations, reflections on the privacy paradox, the impact of external factors, and perspectives on regulatory support as provided through the GDPR. Following this, we present the findings from the follow-up questionnaire study. The participant quotes in the results presentation are translated from Norwegian.

Characteristics of users' data sharing habits

In the interviews, the participants reported varying forms and levels of data sharing when reporting on their habits for sharing of personal data in retail contexts. All participants reported such data sharing, both online and in store. However, there were substantial variations in their willingness to share and the specific contexts of sharing, reflecting convenience-oriented, opportunistic, and risk-oriented approaches.

Convenience-oriented approaches to data sharing

A convenience-oriented approach to data sharing, as reflected in the interviews, may entail a sharing habit where the participants often do not consciously reflect on personal data sharing in concrete retail contexts. Five of the participants reflected a relatively convenience-oriented approach. They considered personal data sharing typically to be a habitual process they engaged in with little or no reflection or afterthought during the actual sharing.

> *"When I buy, or go on websites I do not think too much about what I am clicking on or allow, so I accept cookies and things like that basically every time"* (P12).

The convenience-oriented approach should, however, not necessarily be seen as mindless. Rather, some these participants noted that their habit of being accepting or liberal in their data sharing was grounded in a conscious strategic choice of prioritizing convenience and ease.

> *"I have a conscious but naïve approach to [data sharing] while I believe I mainly am able to avoid the worst."* (P5).

Furthermore, all participants reflecting a convenience-oriented approach to data sharing also indicated situations or contexts where data sharing would not be acceptable to them, such as when providers ask for data highly unrelated to the provided service or in cases of seemingly untrustworthy providers. Also, most of these participants indicated situations where they would have a more strategic or opportunistic approach to data sharing. Among the other participants, one indicated a history of convenience-oriented approach to data sharing, but noted that this was something they had changed.

Opportunistic approaches to data sharing

Opportunistic approaches to personal data sharing was reflected in the interviews as sharing mainly as a means for getting personal benefits, such as discounts for members of customer clubs or access to restricted content, while noting an untroubled attitude towards this habit. As seen in the response from one of the participants,

> *"They can know this about me. Because I have weighed it against me getting a benefit. Even if small. […] I know it can be used in targeted marketing to me. Which I think I can handle."* (P2).

While all but one participants reported on instances of data sharing practices that may be considered opportunistic, five of the participants were found to mainly report on their personal data sharing as opportunistic.

> *"It might be a little weird, maybe I should think it more through, but I think I'm just really quick to just click like okay or accept or what you are clicking. I am just thinking that I am going to the next step, I am getting this discount or get that newsletter, right, and then I just don't think about it"* (P9).

Participant reports suggesting a mainly opportunistic approach to personal data sharing also entailed reports of situations were sharing of such data would not be relevant. That is, these five participants noted that in some contexts the benefits received by data sharing would not outweigh the perceived costs of sharing.

Risk-oriented approaches to data sharing

Risk-oriented approaches to personal data sharing, were identified in the interviews as participants voiced substantial concern regarding sharing of personal data in retail. Four of the participants reflected a markedly risk-oriented approach. Of these, some noted that their privacy concerns had become strengthened over time and that they, in response, actively sought limiting their sharing of personal data, for example with regards to permissions for internet cookies as reflected in this example quote.

> *"In the beginning then the accept cookies, when was it, when it came […] I though okay, it is fine, fine. But now these last six months I have become more conscious that when I am asked to share data, I always press necessary, only necessary data"* (P7).

The risk-oriented participants typically emphasized the negative aspects of personal data sharing, such as issues concerning reduced privacy and the potential for misuse of data. Some also noted their own efforts only to share what is needed of personal data to get required services or voiced a general discomfort associated with sharing of personal data.

> *There is so much information about me out there that I don't want others to have or don't see any need for them to have, and also the constant selling of things, like bombarding me with stuff—that's something I'm not too fond of.* (P13)

Risk-oriented approaches to sharing of personal data were, however, to some extent reported by all the participants

of the study. That is, none of the participants reported to share just any personal data with just anyone. Risk-oriented approaches shared by most of the participants included the need to distinguish between types of personal data and contexts. Most of the participants (11) noted that personal data requested by a provider should be relevant for the particular retail context, and some (6) noted a need to be more restrictive when invited to share personal data considered more sensitive, such as contact information, location, and financial details.

> *"I am very careful with things related to payments, personal identification numbers, and things like that—I am very cautious about those"* (P14).

Most participants (10) further noted that they distinguish between actors worthy or unworthy of their trust for data sharing, and also reported to react negatively on requests for sharing of data not strictly needed for the task at hand.

> *"it is about, what kind of actor it is, and what they need the information for. […] If I, for example, buy something, is it necessary that they know my birthday? […] It is an assessment"* (P3).

Privacy calculations in sharing of personal data

Most participants (10) reported, with some level of detail, to go through a form of calculation prior to deciding whether or not to share personal data with retailers. In this calculation they weighed benefits and costs of sharing.

> *"Yes, I think about it. I am conscious about it, but then I think that it is okay. They get to know this about me, I think, because I have weighed this up against that I get a benefit."* (P6).

Not all reported on going through a privacy calculation prior to sharing data, though. Some noted that they considered sharing of personal data as a requirement to use services they wanted to access or as a means to achieve their objectives in a convenient manner. In consequence, their reports did not indicate a need for making a conscious choice for each instance of data sharing.

> *"But yeah, so I see as, I see sharing the information as necessary to get the service delivered, if that makes sense"* (P10).

Participants reporting to make privacy calculations prior to sharing data varied in terms of the weight they put on benefits and costs on sharing. Some weighed the perceived value higher, accentuating the gains to be made by sharing personal data. Others accentuated the costs of data sharing in terms of the need to give up information of personal relevance, and argued for not sharing data unless the benefit was considered substantial.

> *"I will say no, unless it has a benefit. I do not give just to give, and if I do not get anything out if it."* (P13).

The participants reported on a number of potential negative and positive consequences of data sharing. In the following, we detail the main negative and positive consequences of data sharing reported to be taken into consideration by the participants.

Negative consequences considered in privacy calculations

Key negative consequences reported by the participants to be of relevance for their calculations prior to sharing of personal data in retail, included lack of transparency, a sense of surveillance, and annoyance with advertisement.

Lack of transparency in data sharing was reported as a negative consequence most (13) of the participants took into consideration when considering whether to share personal data. Specifically, the participants noted as problematic that they are not provided sufficient insight into the types of data they are actually sharing nor what the data is used for.

> *"you share a lot of data, you know they know your name, what e-mail address, phone number, possibly which address, which card you are using. And then you do not know much more about what data the application has, what it contains, how long they have the data for"* (P7).

A sense of surveillance, or a feeling of being monitored, was also reported by some (5) as relevant for the participants' data sharing considerations. This sense of surveillance was considered a cause of unease, leading to unwillingness to sharing personal data.

> *"to the degree that I do not wish to share, it is because I do not want unwanted, unnecessary attention on other platforms, other than that I willingly share because I know that I am monitored"* (P1).

Annoyance with advertisement was reported by most participants (8) as a as a third negative consequence considered in privacy calculations. Some of the participants portrayed sharing of personal data as a way to expose oneself to unwanted attention from spammers or marketers, which is illustrated in the following quote.

"There is a lot of information about me out there, that I do not really want anyone to have, or that I do not see a need for them to have, and people constantly selling things, pepper me with things, I am not too fond of that" (P13).

Positive consequences considered in privacy calculations

The participants also reported on positive consequences of data sharing in retail, which made up for the costs represented by the potential negative consequences. These positive consequences included immediate benefits, rewards, and relevant advertisements.

The immediate benefit of data sharing may be an important motivation, as reported by all the participants. In retail, particularly online, sharing of personal data is typically required to conduct desired transactions or get access to desired content.

"I feel like all of the websites I am on have cookies in a way, so there are no websites that do not have it, so then I am like, OK, if I want to go on this website I have to accept" (P11).

Rewards of different forms were also reported by most of the participants (9) as common positive consequences considered as part of decisions on whether or not to share personal data. These rewards could be monetary, for example in the form of discounts or gifts, or informational, in the form of relevant newsletters.

"Like I am selling my personal information, like my, my bank details and my name, my address, but I think that is fine as long as I am getting these, those benefits from this." (P8).

Relevant advertisements were noted by some participants (7) as a third positive consequence of personal data sharing. Indeed, as noted above, advertisement was seen as a potentially negative consequence of sharing personal data for some. However, others saw this as a positive opportunity– as a possible gain, suggesting how the same outcome of data sharing behaviour can be perceived differently between users.

"if I go to Zalando, then I am a little like okay, they can actually give me a personalized offer, if I just click further here, and that is tempting" (P11).

Considerations of trustworthiness in privacy calculations

In addition to considering potential negative and positive consequences in their privacy calculus, some participants also reported on considering risk-related aspects as part of such calculations. Specifically, most participants (12) noted that the business should seem serious and trustworthy for them to share personal data. Such trust could be earned through prior experience or through the brand or word of mouth associated with the business.

"How I decide? No, that depends if I want their service or not? No, so like, I open a website and I choose, and then if they seem credible or trustworthy, and I really would like that cap, for example, then I will buy it and fill in, and I am like, yes, that's it" (P13).

Reflections on the privacy paradox

The participants were not asked directly about the privacy paradox in the study interview guide. However, their responses included numerous indications of the potential relevance of this paradox. These indications could be implicit, where the participants' claims on their own privacy behaviour was contradicted by their other reports on data sharing. But the participants also made explicit notes of seemingly paradoxical approaches to privacy in retail.

Implicit indications of the privacy paradox

Implicit indications of the privacy paradox in retail were interpreted from participants' reports on their data sharing behaviour or in their concerns about data sharing without reflection on potential mitigation actions.

Reports on data sharing behaviour were taken to indicate a privacy paradox in cases where the participants reported on data sharing actions without sufficient corresponding consideration. The participants reported on data sharing behaviour as something potentially requiring attention, while also reporting on not providing this to a sufficient degree.

"I might have some thoughts about it right as I am clicking, or not clicking, but then it kind of just moves along" (P11).

Conversely, participants may also make implicit indications of the privacy paradox as they report unease with specific data sharing behaviour, but without reflecting on potential mitigating behaviours to alleviate their concerns with data sharing.

"I am always thinking about it. It is like, every time I have to write my social security number, I feel this kind of lump in my stomach" (P3).

For some (5), the implicit indications of a privacy paradox suggested a defeatist attitude towards personal data sharing. These participants noted that there seems to be no easy way around data sharing, particularly in online contexts, and one may therefore just as well comply.

"Maybe I could have done more to figure out what the necessary data actually means, though. But then I feel like every website has cookies and then I am like, I feel like I would have to quit using the internet if I found out that I really do not like what the only necessary cookies means and, so yeah, a little difficult honestly" (P11).

Explicit expressions of the privacy paradox

Some of the participants (9) also made explicit expressions of notions or ideas corresponding to the privacy paradox. These participants reported both on the paradoxical practices of consumers in general or on their own paradoxical practices.

For example, one of the participants reflected on the paradoxical data sharing practices in general, noting that people can on the one hand hold a restrictive attitude while on other may display liberal sharing behaviour.

"[we] are the most restrictive and peculiar about what data they want to share, simultaneously we are the most open to share. No, you do not get to know anything about me, because big brother is not allowed to know, oh, do I get coffee? Yes then, go ahead" (P5).

At the individual level, paradoxical practices were suggested as the cause of lack of interest or energy, lack of actual control, or due to the heat of the moment. As noted in the following participant quote.

"Maybe I could have rejected more cookies, but again because I am lazy, it is like this, because I am really actually conscious about it I think, like I try to reject all, but if I am in a bad mood or if I am impatient, then I just click accept, and regret it a little afterwards" (P13).

Factors potentially skewing decisions to share data

The privacy paradox suggests that users' decisions to share data may be skewed by other factors than those accounted for in a privacy calculus. The interviews provided insight into several types of factors that may have such skewing impact, including cognitive factors, emotional factors, social factors, and contextual factors. We detail each of these below.

Cognitive factors

The participants reported on several cognitive factors which might skew their decisions to share data. In particular perceived effort, perceived necessity, and concern for rigged service or interaction design.

Perceived effort of doing adequate calculations prior to sharing data was reported as detrimental by several of the participants (10). These participants expressed that thoroughly assessing implications of data sharing may be difficult to do or highly time consuming. In consequence, they reported to take actions that are less costly in terms of immediate effort required.

"Sometimes there is way too much written, so that if it says click here and share, I just think okay, fine" (P9).

Perceived necessity in data sharing was identified by some (8) as another cognitive factor potentially skewing data sharing decisions. Several of the participants noted that they found sharing of personal data to be the only way to access needed content and services, which in turn lead to a disregard of nuanced calculations.

"It is a little like, if you do not accept these settings, then you will not, then you will not be able to move along, and you really do not have a choice if you want to use the website and the service, so you really just have to accept it" (P4).

Related to the perceived necessity in data sharing noted above, some users (3) voiced a suspicion that design of services may be purposely designed to lead or force users to share personal data. Such perceptions of **rigged service or interaction design** come close to the notion of dark patterns in design and are reflected in the participant quote below.

"No, I don't think I have control over what, what I'm sharing, yeah. I think because this, all this organized and they want data, right? […] it's not actually we decide or, what we want to share, it's actually by them or they want information from us." (P8).

Emotional factors

Emotional factors were also discussed as having the potential to skew user decisions to share personal data. Specifically, the participants reported on liking and trust in the

service provider, as well as positive rapport with individual service personnel.

Personal liking or preferences for a service provider or brand was argued by most participants (10) as a contributor to becoming less concerned regarding privacy and more willing to share personal data. Conversely, a lack of liking or preference could have the opposite effect.

> *"Absolutely you want to share with those you like, or brands you like, rather than brands you do not like, if you do not like them, then I do not know why I would give them information."* (P13).

Positive rapport in the service personnel concerned specific points of contact between the user and the service provider. Some of the participants (3) associated positive rapport with an increase in willingness to comply with requests for sharing personal data while negative rapport entailed the opposite.

> *"Is it a nice, welcoming cashier, it is easier to be nice back and also do the choices they want you to. So absolutely, emotional is a huge factor"* (P4).

Trust in the brand or firm was also mentioned by most participants (12) as a potential emotional factor that could impact their willingness to share personal data. Trust is a complex construct with both emotional and cognitive components. The cognitive aspect of trust has been discussed above. Emotional aspects of trust may likewise be relevant for privacy concerns where, e.g., mere exposure may induce trust and potentially impact willingness to share.

> *"It affects me in a positive way, you get, you become more trusting towards the systems. So it is probably because they are known retailers, stores, brands, then the trust is there."* (P4).

Social and contextual factors

Some of the participants also noted that social and contextual factors could impact their willingness to share personal data in– in retail service contexts as well as in service contexts in general.

Social factors, as noted by most participants (9), could concern explicit advice from friends or family regarding whether or not to share personal data in retail or service contexts. A few participants (2) specifically noted that their willingness to share data with service providers, or to use services for which they would otherwise have privacy concern, could be impacted by their perceptions of what others do or expect from them. This sentiment is illustrated in the following participant quote.

> *[…] so if a friend had told me that he got shampoo or something like that after signing up, then I would have been a bit more willing to do it because I'm influenced by my social environment.* (P11)

Contextual factors, as discussed by some of the participants (6) concerned aspects of the retail environment which could skew their willingness to share personal data in a positive or negative direction. Here, the participants noted that the context of sharing was of substantial importance, as they would assess the relevance or invasiveness of data sharing in part with respect to the service context.

For example, some participants (4) mentioned contexts such as being in a line at checkout as potentially discouraging for sharing of personal data as the presence of others could make the sharing seem more invasive or, also, disrespectful of others.

> *"if there is a long line and there are people behind me, then I am like no, but I can do it later, it is just, I find it uncomfortable"* (P9).

Contextual factors were also mentioned as potentially lowering barriers for sharing personal data. Some participants (6) discussed how a sense of urgency in the retail process could lead them to become less critical in terms of privacy concerns.

"just because it is a big concert, for example, and then it is like first come, first served, and then I am just happy that I got tickets and I do not think about the fact that I have clicked yes" (P12).

Perspectives on regulatory support

Towards the end of the interviews, the participants were enquired concerning their perspectives on regulatory aspects of personal data sharing and how these potentially impacted their own perceptions and practices for data sharing in retail. The participant responses in part concerned their knowledge of privacy regulations and how this might impact them, in part their perceptions of control through regulations.

Knowledge about privacy regulations

Nearly all the participants (13) were aware of privacy regulations. They, however, differed markedly in their knowledge of how these impact sharing and processing of personal data in retail.

Most of the participants (9) reported on knowledge on the GDPR and how it can protect their rights as users, e.g. by giving them rights to insight in the information that they have and concrete penalties if privacy regulations are not adhered to by providers, as well as making the users more conscious about their own sharing habits. Some of the participants also noted an effect on regulation in making users more conscious regarding personal data sharing.

> *"The regulation has made us more conscious, both as a consumer and what responsibility the businesses has"* (P7).

Other participants (5) noted that though they were aware of relevant privacy regulations, they did not have sufficient insight into how this may protect users. Hence, it was seen as difficult to understand the potential impact these might have on their own or others' data sharing.

> *"I have heard about it […], but I have not really put a lot of effort into what it means other than that you have a little more to say in regards to what you want to do, or like, what the data should be used for"* (P11).

Does privacy regulation provide needed control?

The participants also differed markedly in their views of the degree of control they had over their personal data, and the degree to which privacy regulations supported such control.

Half of the participants felt like they had sufficient overview and control over their personal data. In part through their own efforts to keep such control, and in part through a trust in the effect of current data protection regulations.

> *"What I like about the law, for my part, is that it is a set of regulations with concrete regulatory measures supporting my [relaxed data sharing practices]"* (P5).

However, the other half of the participants perceived insufficient control over the personal data they have shared or how this might be processed by service providers. This lack of perceived control led them to express concern.

> *"I don't think I have a good overview of all the information they're collecting […] you can ask, you have the right to ask the information collected to give you, to send you all the data they collect, but you don't I'm not sure if you know how they use data"* (P10).

Results from questionnaire-based follow-up

In the questionnaire-based follow-up study ($N = 191$), participants reported on their approach to sharing of personal data in retail (convenience-oriented, opportunistic, or risk-oriented), their general privacy concern, and their perceptions of the main positive and negative consequences identified as important in privacy calculus in the retail domain.

Approaches to personal data sharing

To identify the participants' main approaches to sharing of personal data in retail, they first responded to statements reflecting the three approaches identified in the interview study (see Appendix). Responses were given on a Likert scale from 1 (disagree strongly) to 7 (agree strongly). Furthermore, in a subsequent question, participants were asked to identify which of the three approaches they most identified with. Participants were identified as particularly reflecting a specific approach to personal data sharing on the basis of their Likert scale response, supplemented with their subsequent self-identification in the case of similar Likert scale scores.

Nearly half the participants were categorized as reflecting a risk-oriented approach to personal data sharing, whereas about a third were categorized as opportunistic and a about a fifth convenience-oriented. Details are provided in Table 1. ANOVAs showed significant differences between the groups in terms of the degree to which they agreed with the statements concerning convenience-oriented ($F(2,183) = 42,4$, $p < ,001$), opportunistic ($F(2,183) = 42,7$, $p < .001$), and risk-oriented ($F(2,183) = 36,3$, $p < ,001$). Tukey HSD with Bonferroni corrections showed significant differences for all pairwise comparisons ($p\text{-}adj < ,05$).

To further verify the grouping of participants as convenience-oriented, opportunistic, and risk-oriented, they were also asked to report on three items measuring privacy

Table 1 Participant categories based on reported approaches to personal data sharing with frequencies as well as mean (*SD*) for participant scores on the statement reflecting the category

Category	Statement in questionnaire	Frequency	Mean (SD)
Convenience-oriented	I share my personal data with retailers when requested, but I don't really think much about it.	42 (22,6%)	5,1 (1,1)
Opportunistic	My personal data are valuable, and I'm willing to share it with retailers if I get something in return.	57 (30,6%)	5,7 (0,8)
Risk-oriented	I'm worried about what retailers might do with my personal data, so I only share it very cautiously.	87 (46,8%)	5,5 (1,3)

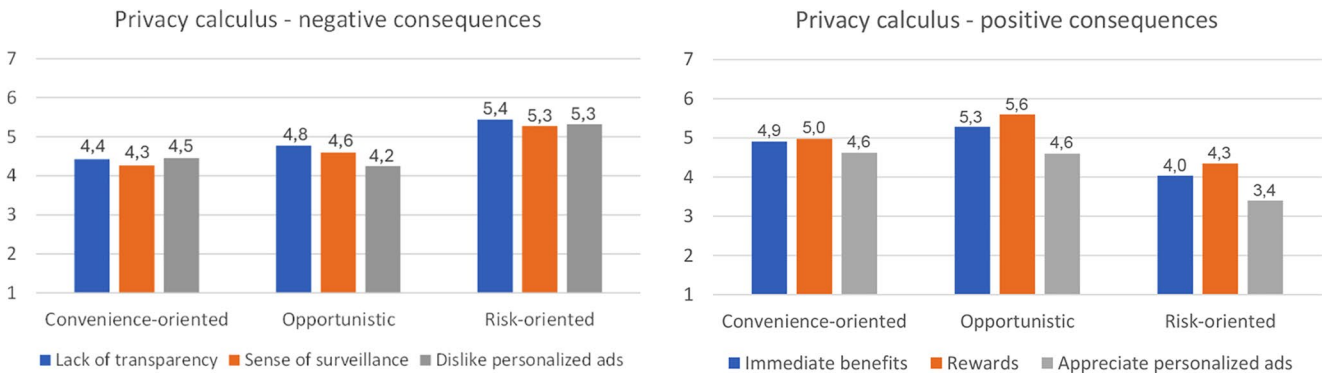

Fig. 1 Overview of scores by participant group for negative and positive consequences considered

concern (see Appendix), adapted from Grosso and colleagues (2020). Responses were given on Likert scales from 1 (disagree strongly) to 7 (agree strongly). The items showed acceptable inter-item reliability (Cronbach alpha = 0,85) and a single measure for privacy concern was established by averaging the participant scores for the three items. Overall, the participants scored 5,1 (SD = 1,2), and 160 (84%) reported agreement with at least one of the items measuring privacy concern. Following ANOVA, the three participant groups reflecting different approaches to sharing of personal data were found to score significantly different on privacy concern ($F(2,183) = 19,7$, p <,001). Pairwise comparisons with Tukey HSD and Bonferroni correction showed significant differences between the risk-oriented and convenience-oriented group (p-adj <,001), as well as the risk-oriented and opportunistic group (p-adj <,001), but not between the convenience-oriented and opportunistic group (p-adj =,29).

Privacy calculus– negative and positive consequences

The participants were asked to respond to six questionnaire items reflecting the three key negative and three key positive consequences considered in privacy calculus, as identified in the interview study. The three key negative consequences were: Lack of transparency in retailer processing of personal data, a sense of surveillance from sharing of personal data in retail, and concern regarding use of personal data for personalized advertising. The three positive consequences were: Immediate benefits following personal data sharing, rewards following personal data sharing, and satisfaction with personalized advertising (see Appendix). Responses were given on a Likert scale from 1 (disagree strongly) to 7 (agree strongly). An overview of the scores of the different participant groups for the different negative and positive consequences are presented in Fig. 1.

Following ANOVA, the three participant groups reflecting different approaches to sharing of personal data were found to score significantly different on privacy concern ($F(2,183) = 19,7, p < .001$). Pairwise comparisons with Tukey HSD and Bonferroni correction showed significant differences between the risk-oriented and convenience-oriented group, as well as the risk-oriented and opportunistic group, for all negative and positive consequences (for all comparisons p-adj <,01). For the convenience-oriented and opportunistic groups, the pairwise comparisons tended towards significance for the positive consequence of rewards (p-adj =,07) but showed non-significant differences for the others (p-adj range =,46 − 1).

Discussion

The presented study provides insight into users' perceptions of personal data sharing and their decision-making process towards such sharing in the retail context. In the discussion section, we will first reflect on these insights relative to existing literature before discussing how these may provide insight in the challenges that HCI researchers could address to reduce users' privacy concerns. Following this, we discuss theoretical and practical implications of the findings, study limitations, and future research.

Characteristics of users' decision-making process for personal data sharing

Variation in retail data sharing habits

The study provides updated insights into perspectives on data sharing and the associated data sharing process. In the interview study, all participants were aware of data sharing in retail on a general level, likely due to the high volumes of personal data sharing and processing in this domain [46]. Furthermore, most participants in the follow-up questionnaire study were in agreement with at least one of the three items measuring privacy concern. This general privacy awareness is well in line with industry reports suggesting increased privacy awareness both from service providers [12] and consumers [14].

At the same time, the interview study also reflect substantial variation between users with regards both to privacy concerns and data sharing habits to be expected in retail. While some participants reported something resembling a fatalist perspective on sharing of personal data, as something one just has to comply with, others were actively seeking means of reducing such sharing or more thoroughly weighing its costs and benefits. Similar variation was observed in the follow-up questionnaire study. This is in line with existing literature, where variation has been shown due to differences in capacity and interest [30] or level of insight [57].

The identified variation in privacy concern also suggests that the cost of being privacy aware may be too high for some. The majority of interview participants indicated that being privacy aware is too consuming in terms of time or effort. This finding is relevant with regards to the notion of privacy resignation, where users due to a sense of disempowerment following from being overwhelmed by myriad privacy decisions, engage in apathetic or cynical data sharing despite a desire to be privacy aware [17, 18].

It is noteworthy that we in our small sample find evidence of three distinct perspectives on data sharing habits in retail. Some participants indicated to prioritize convenience rather than vigilance when reflecting on specific data sharing instances, motivated by an overall acknowledgement of a general need to share data to get needed information and services. Others indicated an opportunistic approach, mainly considering their personal data an asset to be traded for benefits. Yet others, typically reported on a risk-oriented approach expressing substantial privacy concern.

This tripartite distinction of user types– convenience-oriented, opportunistic, and risk-oriented– is interesting both as it echoes privacy segmentation types in the literature– including Westin's [70] distinction between privacy unconcerned, pragmatists, and fundamentalists– and as it suggests different user needs to be addressed through privacy improvements. The user segments identified in the three types may also complement other classifications of users with regards to their privacy concerns. For example, our risk-oriented user type may be seen as particularly concerned with the risk associated with privacy decisions, rather than focussing squarely on privacy as such. Furthermore, our convenience-oriented type seems to strike a balance between Westin's user segment of privacy unconcerned and the alternative user type of privacy cynics suggested by Schomakers and colleagues [60].

Our follow-up questionnaire study indicated substantial prevalence of all three types, though users with a risk-oriented approach were the most prominent group in our sample. The distinction between user types resonates with findings in the literature on privacy concerns as impacted by individual differences, for example in variation in users' propensity to trust [16]. However, the prevalence of risk-oriented users in our study, with nearly half the participants in our follow-up study categorized as belonging to this group, clearly indicates the importance for service providers to facilitate healthy privacy practices. The prevalence of risk-oriented users in our study is also higher than what has been found in other contexts. Westin [70] reported an increase in what he referred to privacy fundamentalists to about one third of the population early in the decade. Schomakers and colleagues [60] identified 38% privacy guardians in their study on online privacy. Recent industry reports also suggest increased privacy awareness in the population [14]. The reason for relatively high prevalence of risk-oriented users found in our study could be due to many aspects of the context. However, it seems to align well with a general tendency towards increased awareness in privacy decision making.

User reports on data sharing decisions in retail

In line with existing knowledge [27], most participants in the interview study typically reported to undertake some form of assessment prior to making decisions on sharing of personal data in the retail context. Here, it is interesting to note that while some of the participants accentuated the need to minimize data sharing, others accentuated the potential positive consequences of data sharing. This duality was corroborated in our follow-up questionnaire study, where the participants categorized as risk-oriented substantially differed from the convenience-oriented and opportunistic participants in their concern for negative consequences of data sharing and views on positive consequences. These dual perspectives on sharing of personal data echoes the argument of Martin and Palmatier [46] of a tension between users' desire for privacy on the one hand and personalization on the other. We find it interesting that each of these two perspectives seem to be voiced more strongly by different participants, where some are more privacy concerned whereas others are more focused on the potential benefits to be had. Potentially, this distinction may allude to a need for privacy management strategies that help users balance benefits and costs, where some may need particular support to take into account the cost whereas others may need support to take into account the benefits.

The participants in the interview study addressed several negative and positive consequences of relevance for a privacy calculus in the retail context. Specifically, lack of transparency, a sense of surveillance, and annoyance with advertisement were given specific mention as negative consequences. Variation in negative consequences is in line with what can be expected from the literature [27], but the specific concerns made are interesting in that they accentuate

aspects of what has been described as surveillance capitalism [76], e.g. in the context of behavioural advertising [73]. Likewise, the positive consequences reported are also aligned with the argument of surveillance capitalism, including immediate benefits, rewards, and relevant advertisements gained from sharing personal data. Hence, while the interview findings clearly suggest a privacy calculus [62], they also reflect key themes in the dystopic perspective of surveillance capitalism [76].

The follow-up questionnaire study further explored the relevance of the negative and positive consequences of relevance for a privacy calculus. Here, it is or particular interest to see how different approaches to personal data sharing may covary with perceptions of negative and positive consequences. Risk-oriented participants were significantly more in agreement with the relevance of negative consequences– lack of transparency, a sense of surveillance, and a dislike for personalized advertisements– than the convenience-oriented and opportunistic participants. Furthermore, opportunistic participants tended towards higher agreement with the relevance of the highest scoring positive consequence– rewards– and were together with the convenience-oriented participants more in agreement with the risk-oriented participants on all three positive consequences– immediate benefits, rewards, and personalized advertisements.

While risk-oriented participants mainly considered negative aspects of such advertising, other participants could be inclined to also see potential benefits. Such findings indicate the need to be respectful of users different preferences and thresholds for what is seen as acceptable use of personal data.

At the same time, our findings illustrate how user's assessments of negative and positive consequences of personal data sharing may imply a need to negotiate conflicting preferences, something that may result in variation in privacy perceptions across contexts. Participants characterized as convenience-oriented and opportunistic reported, on average, resembling scores on dislike of personalized advertising and on perceived benefits of such advertising. This suggests that these user groups may be comfortable with data-driven advertising for some contexts but not for others– a notion that is in line with previous work arguing for the importance of context in users privacy decisions [50, 73]. While categorization of users according to their privacy decision making approaches may support prediction on their privacy decisions, contextual factors will likely also be important in determining such decisions.

The interview reports also indicate substantial awareness of data sharing decisions being impacted by other factors than those included in a privacy calculus. Reported factors were cognitive, emotional, social, and contextual, and correspond well to factors identified in the literature [27]. Furthermore, the interviews also reflected the challenges users may face when trying to be privacy aware. Here, users noted perceptions indicating the relevance of privacy resignation as a potential explanation of personal data sharing practices not in line with what would be expected from a privacy calculus. As noted by Hargittai and Marwick [32, 47], privacy resignation may be a relevant challenge for any user given the challenges of keeping up with privacy decisions– a challenge that is not made easier by the application of dark patterns in privacy design, where users are nudged or forced to share personal data in return for services [28, 29].

This level of awareness in challenges concerning privacy awareness is encouraging, as it suggests that factors potentially skewing a privacy decision-making process may not only be identifiable in research studies [2, 23, 36, 60] but also immediately evident to the individual user. Hence, users may be assumed not just to engage in privacy calculus when sharing data, but also to be able to reflect on their decision-making process and recognize when this breaks down– as suggested in indications of seemingly paradoxical perceptions and behaviours. Hopefully this awareness can be leveraged to encourage needed changes to practices of personal data sharing.

User reports on the benefit of regulation

The participants' levels of awareness concerning privacy regulation is also encouraging, suggesting that users may have some knowledge of regulation though there might be a need for further clarification how to make use of the rights that regulations provide. In their research on internet cookies, Presthus and Sørum [54], showed that users may be aware of beneficial regulation while at the same time may be unable or unwilling to take advantage of such regulation to mitigate privacy issues. Our study complements their findings, though in the specific context of retail, suggesting that users– while typically seeing the benefits of privacy regulation– in part lack insight in the details of how privacy regulation might protect them, and in part lack a sense of control regarding data sharing despite of privacy regulation.

Research challenges for HCI to help reduce users' privacy concerns

Drawing on the user insights from the research, and the reflections of these insights on the basis of the existing knowledge base, we will now reflect on the specific research challenges for the field of HCI that may be relevant to help users in their data sharing decision processes and, thereby reduce privacy concerns.

These reflections are only intended as complementary to other calls for HCI research in the field, including research on privacy implications of user interface design [51], privacy in the internet of things [22], and privacy concerns for vulnerable groups [49]. Specifically, we will address three challenges: scoping, balancing, and acting.

The scoping challenge

Supporting users in scoping their privacy concerns and decisions is an important challenge for HCI. As indicated from the findings of our study, as well as in the research literature, users are challenged to see the full implications of their immediate data sharing decisions. This may be due to the inherent tension between users' desires for relevant services on the one hand, and their desire to protect their privacy on the other [46], as well as the lack of service providers' accommodation of user needs for transparency and simplicity regarding personal data sharing [29]. Furthermore, users may have limited capacity for making privacy calculations [30], or insufficient insight or confidence in how data is processed [57], which may lead to privacy resignation [18] and damage trust in providers [10].

On this background, the immediate benefit achieved from sharing data– such as accessing a service or receiving a reward– may outweigh the concern for long-term negative implications of data sharing. As noted in our findings, participants are particularly concerned about a lack of transparency in data sharing and consequences of data sharing reminiscent of surveillance capitalism [76]. Service providers hence need to put emphasis on simple and transparent information that help users understand the scope of their privacy decisions. HCI research towards this challenge may, e.g., draw on work concerning privacy awareness and privacy by design [24, 41, 55].

The balancing challenge

Building on the first, a second challenge for HCI research is to help users balance costs and benefits in a privacy calculus. As seen in the study findings, users may have different approaches to privacy decisions, where some are convenience-oriented, others opportunistic, and yet others risk-oriented. HCI research is needed to support users with different approaches to decision making to engage in sound data sharing practices.

Helping users to balance benefits and costs in a thoughtful manner, may be particularly challenging for sharing of personal data with varying sensitivity or potential for harm [42]. Hence, helping users to distinguish between data sharing with more or less potential for unwanted implications, will be an important part of the balancing challenge.

The balancing challenge may, in part, be a challenge of user interface design. For example, Fu and colleagues [26] reported on a user-centred process for the design of privacy choice interactions. Following such a line of research, privacy choice interactions could be tailored to suit different user types, or validated as a best fit across user types, drawing on existing research on user-centred design of privacy facts [37, 38] and privacy icons [18, 31], as well as work on user privacy preferences [66, 68]. Furthermore, work on identification and mitigation of dark patterns in privacy design may be important as part of the awareness raising needed to address this challenge properly [28, 29].

In HCI research towards this challenge, it may be beneficial to note users' ability to assess the value of benefits achieved through data sharing [29]. For example, in the retail domain data sharing may have clear and calculable benefits. The balancing challenge requires HCI researchers to facilitate representations of costs in data sharing that are as easy for users to calculate as benefits currently are.

The action challenge

The third challenge we propose as important to accentuate in HCI research, is the action challenge. That is, the challenge of enabling and motivating all users to take sufficient privacy action when engaging with interactive systems and service providers. The findings in the presented study exemplify users' potential for making basic calculations of benefits and costs of data sharing. However, contextual factors may severely skew or bypass this calculation, for example in the form of the social impact of other customers standing in line at a checkout counter or emotional impact of a pleasant interaction, as also shown in the literature [27].

Users, hence, need help in taking concrete steps to support sound privacy decisions amidst contextual distractions. For this, one might, on the one hand, consider design choices that help users make comprehensive considerations when doing data sharing choices [22]. Or one might consider design choices that help users stick to premeditated choices, where they recognize preferrable alternatives, select and move on, or where they, e.g., are supported by context aware [59] or policy driven privacy support [1]. Indeed, a continued challenge for HCI research.

Furthermore, service providers need to be aware of their responsibility in empowering users to take action with regard to privacy protection. The notion of privacy resignation, reflected in our findings of study participants' perceptions of difficulty in engaging in privacy protecting behaviour, may serve as a call to awareness for providers to improve on their personal data collection and related design and information practices.

Implications

While we above have discussed the study findings with regards to how these may inform the field of HCI research with regards to key challenges in user-centred design of privacy choice, the study also has some general implications which we briefly summarize here. These implications concern theory and practice.

Implications for theory

In addition to the proposed HCI challenges, the study holds the following two theoretical implications.

Users' privacy awareness In response to Martin and Palmatier's [46] call for research shedding light on users' insight into sharing of personal data and its implications, we have provided a qualitative exploration with a quantitative follow-up showing the potential that users may have for insightful and informed choice, in line with a privacy calculus, as well as an awareness of factors that might limit their ability to make informed choices. Here, we note that the efforts required to be privacy aware may need even more attention in the literature to ensure that privacy awareness enables action instead of inducing resignation [17].

Individual variation in users' approaches to privacy decisions The study suggests a tripartite classification of users, with reports of convenience-oriented, opportunistic, and risk-oriented approaches to privacy decisions. The relevance of the classification has been initially tried in the follow-up questionnaire study. Potentially this classification could form the basis for a user typology to support future privacy design work, complementing existing typologies from privacy segmentation research [60, 70].

Implications for practice

The study also holds implications for practice. We find the following four to be of particular relevance.

Improve support for privacy decision making Our study findings show that while users may be privacy concerned, the resource demand for acting on this may be too high. At the same time, privacy awareness is likely on the rise [14]. Service providers may, hence, benefit, in terms of improved user experience or trust [10], for strengthening support for privacy decision making.

Cater to variation in users' needs Users vary in their needs for support during privacy decisions. Different user types may have different requirements, and service providers aiming to provide optimal support for privacy decision making needs to do this in a user-centred manner fitting different users' needs.

Mind opportunistic privacy decisions Users displaying an opportunistic approach to privacy decision making may be valuable to achieve an improved basis for understanding the process of privacy decision-making. Opportunistic calculation of benefits for sharing personal data may pave the way for more comprehensive assessment including nuanced considerations of benefits and costs, potentially leading to strengthened expectations for accountability in service providers.

Foster provider responsibility The substantial share of users categorized as risk-oriented in the study, along with the increased demands on providers following from privacy legislation and users' associated awareness of this legislation, suggests a need for further fostering of privacy responsibility among service providers. Such responsibility should entail support for helping users engaging in healthy privacy decisions, as well as striving for transparency and accountability in person data collection and use.

Limitations and future research

The presented study is a small-scale exploration of an important research area. While the explorations have enabled in-depth insight into users current decision-making process in a specific domain and thereby allowed for reflection on key privacy research challenges for HCI, the study has important limitations.

First, the study is limited as it is conducted on a relatively small scale in a specific market. While the study allows interesting insights, it will be highly interesting to see similar exploratory studies in other domains and markets. Such replications of the study may provide a richer understanding of users' decision-making processes for sharing of personal data and may help expand on the proposed research challenges.

Second, the study is limited as it only concerns users' self-reports and reflections on sharing of personal data, and

not data on user behaviour. While the study provides useful insight into users' reflections and perspectives on privacy and data sharing, this insight would have been further strengthened through triangulation with behavioural data. We foresee future research to include data on users' behaviour to complement self-reports.

Third, the study is limited as it only proposes research challenges for the field of HCI without proposing concrete steps towards addressing these challenges. Such proposals of steps to address the research challenges could, for example, be gathered through involvement of a broader range of researchers in the process. We nevertheless believe the challenges will be helpful starting points for discussion and reflection in the field and hope that they will motivate needed future research in this important area.

Appendix

Measurement instruments used in the follow-up questionnaire study.

Approach to personal data sharing

Approach to personal data sharing was measured by the following three items, scored on a Likert scale from 1 (disagree strongly) to 7 (agree strongly).

- I share my personal data with retailers when requested, but I don't really think much about it.
- My personal data are valuable, and I'm willing to share it with retailers if I get something in return.
- I'm worried about what retailers might do with my personal data, so I only share it very cautiously.

Following their response to the three items, the participants were requested to select which of the three items that described them the most.

Participants were divided in three groups of different approaches to personal data sharing based on their responses. Participants who scored higher on one of the Likert scale items than the two others were designated to the corresponding group. Participants with two or three highest storing items were designated to a group based on their selection of which of the three items that described them the most. In this second steps, participants with selection of items that described them the most not matching a highest-scoring Likert scale item were filtered out (5 participants).

Privacy concern

Privacy concern was measured by the following three items adapted from Grosso et al. [21], scored on a Likert scale from 1 (disagree strongly) to 7 (agree strongly).

- When retailers ask me for personal information, I sometimes think twice before providing it.
- It bothers me that I need to give personal information to many retailers.
- I am concerned that retailers are collecting too much personal information about me.

Privacy calculus– negative consequences considered

Participants were asked to respond to the following three items reflecting the three key negative consequences considered in privacy calculus, as identified in the interview study. The items were scored on a Likert scale from 1 (disagree strongly) to 7 (agree strongly).

- I am concerned about a lack of transparency in collection and use of personal data by retailers.
- I am concerned about a sense of surveillance that comes from sharing personal data with retailers.
- I am concerned about how personal data is used by retailers to personalize advertisement to me.

Privacy calculus– positive consequences considered

Participants were asked to respond to the following three items reflecting the three key positive consequences considered in privacy calculus, as identified in the interview study. The items were scored on a Likert scale from 1 (disagree strongly) to 7 (agree strongly).

- I like the immediate benefits that can follow from sharing my personal data with retailers.
- I like getting rewards for sharing my personal data with retailers.
- I like that data sharing with retailers can make advertisements more personalized.

Funding Open access funding provided by SINTEF

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

1. Ackerman M, Darrell T, Weitzner DJ (2001) Privacy in context. Human–Computer Interact 16(2–4):167–176
2. Acquisti A, Adjerid I, Balebako R, Brandimarte L, Cranor LF, Komanduri S, Leon PG, Sadeh N, Schaub F, Sleeper M, Wang Y, Wilson S (2017) Nudges for privacy and security: Understanding and assisting users' choices online. ACM-CSUR 50(3):1–44
3. Aguirre E, Mahr D, Grewal D, De Ruyter K, Wetzels M (2015) Unraveling the personalization paradox: the effect of information collection and trust-building strategies on online advertisement effectiveness. J Retail 91(1):34–49
4. Alfnes F, Wasenden OC (2022) Your privacy for a discount? Exploring the willingness to share personal data for personalized offers. Telecomm Policy 46(7):102308
5. Barnes SB (2006) A privacy paradox: social networking in the united States. First Monday 11(9). https://doi.org/10.5210/fm.v11i9.1394
6. Beke FT, Eggers F, Verhoef PC, Wieringa JE (2022) Consumers' privacy calculus: the PRICAL index development and validation. Int J Res Mark 39(1):20–41
7. Bongard-Blanch K, Rossi A, Rivas S, Doublet S, Koenig V, Lenzini G (2021) I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!—Dark Patterns from the End-User Perspective. In Proceedings of the 2021 ACM Designing Interactive Systems Conference (DIS '21), ACM, New York, NY, pp. 763–776
8. Borgesius FJZ, Kruikemeier S, Boerman SC, Helberger N (2017) Tracking walls, Take-It-Or-Leave-It choices, the GDPR, and the ePrivacy regulation. Eur Data Prot Law Rev 3(3):353–368
9. Braun V, Clarke V (2006) Using thematic analysis in psychology. Qualitative Res Psychol 3(2):77–191
10. Bughin J (2011) Digital user segmentation and privacy concerns. J Direct Data Digit Mark Pract 13:156–165
11. Cheah JH, Lim XJ, Ting H, Liu Y, Quach S (2022) Are privacy concerns still relevant? Revisiting consumer behaviour in omnichannel retailing. J Retailing Consumer Serv 65:102242
12. Chen HT (2018) Revisiting the privacy paradox on social media with an extended privacy calculus model: the effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. Am Behav Sci 62(10):1392–1412
13. Cisco (2023) Consumer Privacy Survey Report. https://www.cisco.com/c/en/us/about/trust-center/consumer-privacy-survey.html
14. Cisco (2024) Data Privacy Benchmark Study. https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html
15. Dienlin T (2023) Privacy calculus: Theory, studies, and new perspectives. In The Routledge Handbook of Privacy and Social Media, Routledge, pp. 70–79
16. Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Privacy calculus model in e-commerce– a study of Italy and the united States. Eur J Inform Syst 15:389–402
17. Draper NA (2017) From privacy pragmatist to privacy resigned: challenging narratives of rational choice in digital privacy debates. Policy Internet 9(2):232–251
18. Draper NA, Hoffmann CP, Lutz C, Ranzini G, Turow J (2024) Privacy resignation, apathy, and cynicism: introduction to a special theme. Big Data Soc 11(3):1–9
19. Dupree JL, Devries R, Berry DM, Lank E (2016) Privacy personas: Clustering users via attitudes and behaviors toward security practices. In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ACM, pp. 5228–5239
20. Efroni Z, Metzger J, Mischau L, Schirmbeck M (2019) Privacy icons: A risk-based approach to visualisation of data processing. Eur Data Prot Law Rev 5:352–366
21. Egelman S, Peer E (2015) The myth of the average user: Improving privacy and security systems through individualization. In Proceedings of the 2015 New Security Paradigms Workshop–NSPW'15, ACM Digital Library, pp. 16–28
22. Feng Y, Yao Y, Sadeh N (2021) A design space for privacy choices: Towards meaningful privacy control in the internet of things. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, New York, NY, pp. 1–16
23. Fernandes T, Pereira N (2021) Revisiting the privacy calculus: why are consumers (really) willing to disclose personal data online? Telematics Inform 65:101717
24. Fischer-Hübner S, Angulo J, Pulls T (2014) How can cloud users be supported in deciding on, tracking and controlling how their data are used? Privacy and identity management for emerging services and technologies. Springer, Berlin, pp 77–92
25. Fox G, Lynn T, Rosati P (2022) Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. Inform Technol People 35(8):181–204
26. Fu J, Zhang J, Li X (2023) How do risks and benefits affect user' privacy decisions? An event-related potential study on privacy calculus process. Front Psychol 14:1052782
27. Gerber N, Gerber P, Volkamer M (2018) Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers Secur 77:226–261
28. Gray CM, Chen J, Chivukula SS, Qu L (2021) End user accounts of dark patterns as felt manipulation. In Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2): 1–25
29. Gray CM, Kou Y, Battles B, Hoggatt J, Toombs AL (2018) The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, New York, pp. 1–14
30. Grosso M, Castaldo S, Li HA, Larivière B (2020) What information do shoppers share? The effect of personnel-, retailer-, and country-trust on willingness to share information. J Retail 96(4):524–547
31. Habib H, Zou Y, Yao Y, Acquisti A, Cranor L, Reidenberg J, Schaub F (2021) Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. ACM, New York, pp. 1–25
32. Hargittai E, Marwick A (2016) What can I really do? Explaining the privacy paradox with online apathy. Int J Communication 10:3737–3757
33. Hoofnagle CJ, Urban JM (2014) Alan westin's privacy homo economicus. Wake for Law Rev 49:261–317
34. Ismagilova E, Hughes L, Rana NP, Dwivedi YK (2022) Security, privacy and risks within smart cities: literature review and development of a smart City interaction framework. Inform Syst Front:1–22
35. Joinson AN, Reips UD, Buchanan T, Schofield CBP (2010) Privacy, trust, and self-disclosure online. Human–Computer Interact 25(1):1–24

36. Kehr F, Wentzel D, Kowatsch T, Fleisch E (2015) Rethinking privacy decisions: pre-existing attitudes, pre-existing emotional states, and a situational privacy calculus. Proceedings of ECIS 2015, AIS Electronic Library
37. Kelley PG (2013) Designing privacy notices: supporting user Understanding and control. Carnegie Mellon University
38. Kelley PG, Cranor LF, Sadeh N (2013) Privacy as part of the app decision-making process. In Proceedings of the SIGCHI conference on human factors in computing systems, ACM, New York, pp. 3393–3402
39. Kokolakis S (2017) Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers Secur 6:122–134
40. Langheinrich M (2001) Privacy by design—principles of privacy-aware ubiquitous systems. In International conference on ubiquitous computing, Springer, Berlin, pp. 273–291
41. Leschanowsky A, Popp B, Peters N (2023) Privacy strategies for conversational AI and their influence on users' perceptions and decision-making. In Proceedings of the 2023 European Symposium on Usable Security, pp. 296–311
42. Li S, Li R, Zhu B, Zhang B, Li J, Liu F, Wei Y (2023) Research on user's highly sensitive privacy disclosure intention in home intelligent health service system: A perspective from trust enhancement mechanism. Digit Health 9:20552076231219444
43. Marriott HR, Williams MD, Dwivedi YK (2017) Risk, privacy and security concerns in digital retail. Mark Rev 17(3):337–365
44. Martin K, Nissenbaum H (2016) Measuring privacy: an empirical test using context to expose confounding variables. Columbia Sci Technol Law Rev 18:176–218
45. Martin K (2018) The penalty for privacy violations: how privacy violations impact trust online. J Bus Res 82:103–116
46. Martin KD, Palmatier RW (2020) Data privacy in retail: navigating tensions and directing future research. J Retail 96(4):449–457
47. Marwick A, Hargittai E (2019) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. Inform Communication Soc 22(12):1697–1713
48. Milne GR, Bahl S (2010) Are there differences between consumers' and marketers' privacy expectations? A segment-and technology-level analysis. J Public Policy Mark 29(1):138–149
49. McDonald N, Forte A (2020) The politics of privacy theories: Moving from norms to vulnerabilities. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, New York, pp. 1–14
50. Nouwens M, Liccardi I, Veale M, Karger D, Kagal L (2020) Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI conference on human factors in computing systems, ACM, New York, pp. 1–13
51. Okazaki S, Eisend M, Plangger K, de Ruyter K, Grewal D (2020) Understanding the strategic consequences of customer privacy concerns: A meta-analytic review. J Retail 96(4):458–473
52. Pizzi G, Scarpi D (2020) Privacy threats with retail technologies: A consumer perspective. J Retailing Consumer Serv 56:102160
53. Presthus W, Sønslien KF (2021) An analysis of violations and sanctions following the GDPR. Int J Inform Syst Project Manage 9(1):38–53
54. Presthus W, Sørum H (2019) Consumer perspectives on information privacy following the implementation of the GDPR. Int J Inform Syst Project Manage 7(3):19–34
55. Prillard O, Boletsis C, Tokas S (2024) Ethical design for data privacy and user privacy awareness in the metaverse. In Proceedings of the 10th International Conference on Information Systems Security and Privacy, SciTePress, pp. 333–341
56. Quach S, Barari M, Moudrý DV, Quach K (2022) Service integration in omnichannel retailing and its impact on customer experience. J Retailing Consumer Serv 65:102267
57. Riegger AS, Klein JF, Merfeld K, Henkel S (2021) Technology-enabled personalization in retail stores: Understanding drivers and barriers. J Bus Res 123:140–155
58. Rogers EM (2003) Diffusion of Innovations (5th edition). Free Press, New York
59. Schaub F, Könings B, Weber M (2015) Context-adaptive privacy: leveraging context awareness to support privacy decision making. IEEE Pervasive Comput 14(1):34–43
60. Schomakers EM, Lidynia C, Ziefle M (2019) A typology of online privacy personalities: exploring and segmenting users' diverse privacy attitudes and behaviors. J Grid Comput 17(4):727–747
61. Schweidel DA, Bart Y, Inman JJ, Stephen AT, Libai B, Andrews M,… Thomaz F (2022)How consumer digital signals are reshaping the customer journey. Journal of the Academy of Marketing Science 50(6):1257–1276
62. Smith HJ, Dinev T, Xu H (2011) Information privacy research: an interdisciplinary review. MIS Q 35(4):989–1015
63. Solove DJ (2021) The myth of the privacy paradox. George Wash Law Rev 89(1)
64. Statista (2024) Online grocery shopping behavior– statistics & facts. https://www.statista.com/topics/4876/us-online-grocery-shopping-consumer-behavior
65. Statistics Norway (2024) ICT usage in households. https://www.ssb.no/en/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/bruk-av-ikt-i-husholdningene
66. Tøndel IA, Nyre ÅA, Bernsmed K (2011) Learning privacy preferences. In Proceedings of the International Conference on Availability, Reliability and Security, IEEE, pp. 621–626
67. Trepte S, Scharkow M, Dienlin T (2020) The privacy calculus contextualized: the influence of affordances. Comput Hum Behav 104:106115
68. Wijesekera P, Reardon J, Reyes I, Tsai L, Chen JW, Good N,… Egelman S (2018) Contextualizing privacy decisions for better prediction (and protection). In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, New York, pp. 1–13
69. Watson J, Lipford R, Besmer A (2015) Mapping user preference to privacy default settings. ACM Trans Computer-Human Interact (TOCHI) 22(6):1–20
70. Westin AF (2003) Social and political dimensions of privacy. J Soc Issues 59(2):431–453
71. Woodruff A, Pihur V, Consolvo S, Brandimarte L, Acquisti A (2014) Would a privacy fundamentalist sell their {DNA} for {$1000… If} nothing bad happened as a result?The Westin categories, behavioral Intentions, and consequences. In 10th Symposium on Usable Privacy and Security– SOUPS 2014, pp. 1–18
72. Wu Y, Bice S, Edwards WK, Das S (2023) The slow violence of surveillance capitalism: How online behavioral advertising harms people. In Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency, ACM, New York, pp. 1826–1837
73. Yang Y, Li TW, Jin H (2024) On the feasibility of predicting users' privacy concerns using contextual labels and personal preferences. In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems– CHI '24, ACM, New York, pp. 1–20
74. Yeung K (2018) Five fears about mass predictive personalization in an age of surveillance capitalism. Int Data Priv Law 8(3):258–269
75. Zhang D, Boerman SC, Hendriks H, van der Goot MJ, Araujo T, Voorveld H (2024) They know everything: folk theories, thoughts, and feelings about dataveillance in media technologies. Int J Communication 18:2710–2730
76. Zuboff S (2019) The age of surveillance capitalism. Profile Books, London

77. Zuboff S (2022) Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. Organ Theory 3(3):26317877221129290