A Qualitative Model of Older Adults' Contextual Decision-Making About Information Sharing

ALISA FRIK, International Computer Science Institute; University of California, Berkeley
JULIA BERND, International Computer Science Institute; University of California, Berkeley
NOURA ALOMAR, University of California, Berkeley
SERGE EGELMAN, International Computer Science Institute; University of California, Berkeley

The sharing of information between older adults and their friends, families, caregivers, and doctors promotes a collaborative approach to managing their emotional, mental, and physical well-being and health, prolonging independent living and improving care quality and quality of life in general. However, information flow in collaborative systems is complex, not always transparent to elderly users, and may raise privacy and security concerns. Because older adults' decisions about whether to engage in information exchange affects interpersonal communications and delivery of care, it is important to understand the factors that influence those decisions. While a body of existing literature has explored the information sharing expectations and preferences of the general population, specific research on the perspectives of older adults is less comprehensive. Our work contributes empirical evidence and suggests a systematic approach. In this paper, we present the results of semi-structured interviews with 46 older adults age 65+ about their views on information collection, transmission, and sharing using traditional ICT and emerging technologies (such as smart speakers, wearable health trackers, etc.). Based on analysis of this qualitative data, we develop a detailed model of the contextual factors that combine in complex ways to affect older adults' decision-making about information sharing. We also discuss how our comprehensive model compares to existing frameworks for analyzing information sharing expectations and preferences. Finally, we suggest directions for future research and describe practical implications of our model for the design and evaluation of collaborative information-sharing systems, as well as for policy and consumer protection.

Additional Key Words and Phrases: information sharing, data flows, older adults, interviews

Citation:
Alisa Frik, Julia Bernd, Noura Alomar, and Serge Egelman. 2020. A Qualitative Model of Older Adults' Contextual Decision-Making About Information Sharing. Proceedings of the 20th Annual Workshop on the Economics of Information Security (WEIS 2020), Brussels, Belgium, December 14–15, 2020. 62 pages.

1 INTRODUCTION

Older adults' essential everyday needs are often met through technology. In particular, the COVID-19 pandemic has led to heavier reliance on technology for grocery and other shopping, communication, entertainment, and emotional support. By 2030, 1 in 5 US residents is projected to reach the retirement age of 65 years or older [108]. The expansion of the population of older adults will bring additional challenges associated with addressing their everyday needs, including physical and mental health needs [79]. Information and communication technologies (ICT) can facilitate

Authors' addresses: Alisa Frik, afrik@icsi.berkeley.edu, International Computer Science Institute; University of California, Berkeley; Julia Bernd, jbernd@icsi.berkeley.edu, International Computer Science Institute; University of California, Berkeley; Noura Alomar, nnalomar@berkeley.edu, University of California, Berkeley; Serge Egelman, egelman@icsi.berkeley.edu, International Computer Science Institute; University of California, Berkeley.

service provision and reduce the cost of care [82], prolong independent living, and improve overall well-being.

Building systems that rely on efficient information flows and foster collaborative cultures between elderly users, and their friends, family members, and caregivers requires paying particular attention to making those information flows transparent to all stakeholders. Lack of transparency in such systems could introduce potential barriers to technology adoption [25, 32, 37, 49], as it may raise privacy and security concerns among older adults. Moreover, prior work has found that older adults have granular, context-dependent preferences about information sharing [90]. Failure to address these concerns and contextual preferences may negatively impact the potential of ICT to improve the level of cooperation and information sharing between elderly patients and their caregivers. For instance, lack of effective communication could result in less accurate diagnoses, delayed medical attention, or feelings of loneliness and abandonment.

In this paper, we examine the factors that drive older adults' decisions about whether to engage in information exchange, based on analysis of semi-structured interviews with 46 older adults aging 65 years and older. The interviews explored participants' views on information collection, transmission, and sharing using traditional ICT (smartphones, tablets, computers) and emerging technologies (such as smart speakers, wearable health trackers, etc.).

Our analysis found that opinions of older adults about whether to share their information are highly context-dependent and involve weighing complex trade-offs. Our empirical findings contribute to a growing body of research showing that users' attitudes, preferences, and behaviors regarding information-sharing in general and privacy and security specifically are complex, dynamic, and context-dependent [e.g., 2, 12, 58, 66, 76, 90**?**].

Such heterogeneous and nuanced judgments invite a systematic approach to representing the contextual factors involved. In our data, even common judgments about seemingly straightforward paradigm examples (e.g. of sensitive data types or trusted recipients) were illuminated by examining them in terms of implicit underlying factors.

The central contribution of this paper is therefore our proposal of a comprehensive model of factors affecting the context-specific decision-making of older adults about information sharing. The proposed model encompasses a broad range of decision-making factors that we categorize under seven dimensions: decision maker, data, recipients, purposes and benefits, risks, system, and environment.

As with most qualitative research, the findings are based on interviews with a limited sample of participants. We do not attempt to estimate the prevalence of preferences or relative impact of factors on decision-making; however, based on comparison with prior research with other populations and in other contexts, we believe that our model can be generalized to broader populations of older adults in the US. In future work, we plan to quantify our findings and validate the model with a broader population of participants, including younger and older adults, and with diverse socioeconomic and demographic characteristics.

Once validated, our model could provide the foundation for a generalized model of sharing decisions across populations, which could then be used in comparison studies. Without a solid theoretical foundation and a systematic taxonomy and model of factors and sub-factors, empirical studies are difficult to replicate and compare, and their results are difficult to consolidate and use for further advancement of knowledge—or for improvement of real-world practices in the field.

In developing such a broad, structured model, we also hope to lay the groundwork for tying together various existing theories that focus in depth on specific dimensions of sharing decisions. Existing theoretical frameworks addressing privacy decision-making are scarce and disconnected, are incomplete due to focusing in-depth on specific factors of interest, or lack guidelines for practical applications (see §2).

In addition, our findings have practical implications for technology development, education, and policy. By supporting a better understanding of information-sharing behaviors and decision-making, and underlying attitudes and preferences, future research using our model can inform product design and data regulations, and thus improve data protection. In the long term, educating developers about consumer expectations can encourage a shift in norms towards a safer and more privacy-respecting online ecosystem, while at the same time, educating consumers can inform their privacy expectations and improve their safety.

Organization. The rest of the paper is organized as follows. In §2, we begin by reviewing theoretical literature on privacy decision-making and empirical studies of data sharing preferences of the population in general and older adults in particular. We then describe our research methodology and participant characteristics in §3 and §4. In §5, we present high-level findings about how our participants approach privacy decisions, and in §6, we present our comprehensive model of factors describing older adults' data sharing decisions. We then discuss the theoretical and practical implications of our model and conclude the paper, in §7 and §8, respectively.

2 RELATED WORK

In this section, first we review the empirical evidence aiming at illustrating users' data sharing decisions, then, we review theoretical frameworks aiming at explaining and modeling such decisions.

2.1 Empirical Evidence

In this section, we review the empirical evidence that focuses on studying users' (including elderly users') privacy expectations and sharing preferences and decisions when using traditional (computers, tablets, smartphones) and emerging (smart speakers, wearable trackers, smart TVs, etc.) technologies.

2.1.1 Data Sharing Preferences of the General Population. There has been a large body of work that studied users' privacy attitudes, preferences and expectations in different contexts, such as e-commerce scenarios, healthcare contexts, and smart homes [1, 64, 97, 120]. Based on his prior interviews, focus groups, and surveys about users' privacy perceptions of three multimedia communication environments (virtual reality, video conferencing, and Internet multicasting), Adams [3] developed a model in which three major privacy factors—information receivers (mediated by trust), potential usage of collected data (affecting risk/benefit trade-offs), and information sensitivity—affect users' perceptions of privacy in multimedia communications. He acknowledges that context affects users' perceptions, but does not elaborate on what defines the context and how it impacts the perceptions.

Lederer et al. [64] designed a questionnaire-based study to evaluate the relative importance of two of the factors identified by Adams [3], namely data recipient and the context, on the preferred accuracy of personal information disclosed through a mobile phone. Lederer et al. [64] found that data recipients are stronger predictors of privacy decisions than disclosure context, whereas users are more likely to disclose information to the same recipient in different contexts than to disclose it to different recipients in the same context. Lau et al. [62], in interviews with smart speaker users, found that many of them do not perceive privacy risks associated with using always-listening devices and trust smart speaker manufacturers in protecting their privacy.

Focusing on IoT-related privacy concerns, Naeini et al. [85] surveyed over 1000 participants in a vignette-based study and identified perceived benefits, types of collected data, and users' beliefs about third-party sharing as important factors that affect users' data sharing decisions in IoT contexts. Lee et al. [66] in a large-scale survey-based study investigated the privacy expectations surrounding the use of wearable devices. They found that users are concerned about the privacy and security risks associated with using technologies that collect or store their financial information or video recordings of them. In contrast, with respect to fitness data specifically, Alqhatani and Lipford's [6] interview study found that participants' sharing decisions were goal-driven, and that they were more concerned about managing self-presentation than (other) privacy or security risks.

Naeini et al. [86] presented different hypothetical IoT-based data collection scenarios to participants on Mechanical Turk and found that certain social cues, such as the data-sharing decisions of friends (i.e., denying or allowing data collection), can impact users' privacy decisions. Wiese et al. [111] found that certain aspects of relationships between connections ('friends') on Facebook's social media platform, such as frequency of communication and tie strength (closeness), affect users' decisions to share information with those connections.

The results described above show potential in predicting users' information sharing decisions. For instance, Bilogrevic et al. [18] used a machine learning algorithm, SPISM, to predict at what granularity the user will be willing to share their personal information. The predictive algorithm relied on 18 features in 7 categories: 'person' (including user's familiarity and social ties with the recipient), 'service' category, 'what?' (including request type and details), 'location', 'when?' (including time, weekday, daytime, and activity), 'with whom?' (including neighbors and neighbors type), and 'last interaction' details. In the experiment, this algorithm achieved 90% accuracy in predicting sharing decisions. The accuracy of these systems greatly depends on having more accurate models to predict users' data-sharing preferences and expectations, which is the main motivation for our work.

2.1.2 Data Sharing Preferences of Older Adults. Some prior work has specifically explored the determinants of data sharing decisions of older adults in a number of contexts, including social media and smart homes [16, 26, 50, 68, 69, 78, 113]. For instance, a perceived need for technology and lack of awareness of privacy risks have been shown to affect older adults' data sharing decisions [19, 69]. Lorenzen-Huber et al. [69] conducted focus group sessions with 64 older adults and found that older adults' privacy concerns are negatively associated with perceived usefulness of in-home monitoring technologies (for the current need, not preventative use), and positively associated with the perceived sensitivity and granularity of data collected by such technologies. They were also concerned that high granularity may increase the undesirable burden of caregiving. Participants expressed a desire to maintain granular control over what information is shared and with whom, as personal relationship and trust levels differ among various family caregivers.

Other studies also showed a significant role of data recipients on information sharing decisions. For instance, older adults have been shown to feel comfortable sharing their data with their doctors [16, 113]. Similarly, Boise et al. [19] found that 72% of older adults are willing to share data collected by healthcare monitoring systems with caregivers and family members, but are concerned about data sharing with unintended parties. Xing et al. [116] conducted five focus groups with seniors and some of their family members to understand the challenges that hinder the adoption of wearable medical devices by elderly people. Many participants were worried that the health data collected by wearable devices would not be adequately protected and might therefore be subject to misuse by data recipients. Mynatt et al. [84] observed that seniors prefer limiting access to their data to a small group of family members and that they value technologies that collect or share their data only when necessary (e.g., in emergency situations).

When the perceived usefulness becomes a necessity, older adults are likely to trade their privacy for large benefits, such as "aging in place," i.e., living independently in their homes (e.g., by utilizing in-home monitoring technologies) [16, 60, 113]. Poor health conditions also make users more likely to accept the privacy trade-off. For example, Beach et al. [16] found that disabled adults were more willing to share their information compared to non-disabled adults. Courtney et al. [33] found that older adults' perceived need for a technology is likely to override their privacy preferences. This is consistent with prior findings [60, 81, 82], which highlight that perceived benefits of using a technology are more important than the costs associated with adopting the technology.

Nevertheless, a few research efforts have suggested that older adults' privacy concerns are potential barriers to technology adoption [25, 32, 37]. For instance, Demiris et al. [36], in focus groups with 14 seniors, found that older adults have privacy concerns that might affect their adoption of sensor-based smart home technologies. This study also found that older adults demand features that allow them to access the sensor data collected by smart home technologies and specify the recipients who are allowed to access the collected data [36]. This body of research suggests that implementing user controls over the information flows is vital for the market success of data-driven collaborative systems.

2.2 Theoretical Frameworks

A number of theoretical frameworks explain particular aspects of users' data sharing decisions; the most relevant include the Theory of Privacy as Contextual Integrity [87–89], Communication Privacy Management Theory [92, 93], Altman's Boundary Regulation Theory [8, 91, 102], Protection Motivation Theory [98], and Privacy Calculus Theory [39]. In this section we review the most relevant theoretical frameworks and outline their limitations in terms of depth or breadth of scope necessary for their successful operationalising.

One of the most prominent frameworks focused on contextual factors is the Theory of Privacy as Contextual Integrity (CI) [87–89]. CI predicts that privacy violations occur when an information exchange does not conform to the established contextually-specific norms about information flow [e.g., 12, 14, 22, 76, 87, 88]. CI outlines 5 contextual parameters describing information transfers: data subject, sender, recipient, attribute (i.e. information type, topic, or content of the data), and transmission principles (how the data is shared, or under what conditions).

While CI is a useful analytical framework for assessing *the perceived appropriateness* of a specific data flow, it does not describe the complex array of other factors—beyond predicted appropriateness—that individual users take into account in privacy *decision making*. Moreover, CI provides little guidance about what specifically constitutes the transmission principles and how they affect the norms of sharing.

Communication Privacy Management Theory (CPM, or Communication Boundary Management Theory) [75, 92, 93] also includes in its model the contextual factors that affect how people form information disclosure rules and draw boundaries between public and private information. The failure of recipients to effectively negotiate or follow privacy rules results in privacy violations. According to CPM, privacy rules are formulated based on gender, cultural norms, context, motivation, and risk/benefit ratio. Context includes physical and social environments such as family, health, or work communication environments. CPM also accounts for how privacy boundaries change during the life span. However, CPM does not further specify what in particular defines a given context.

Similarly, Altman's Boundary Regulation Theory (BRT) [7, 8] holds that privacy is not static and does not have universal rules, but is a dynamic, situationally specific, and selective process of boundary regulation and control of access to the self. A person's desired level of privacy is continuously changing along a continuum between openness and closeness in response to situational factors and circumstances, such as cultural practices and social relationships and processes, along with more general individual tendencies [8, 91, 102]. BRT focuses on balancing intrusion avoidance and loneliness avoidance, but does not consider a variety of other goals the decision maker may have, such as seeking help in emergency situations, sharing the knowledge for societal benefits or research, or avoiding sharing the information that may disappoint the recipient.

Protection Motivation Theory [98] and Technology Threat Avoidance Theory [67] posit that users' decisions to avoid privacy-related threats are determined by their perceptions of how likely they are to experience such threats, the level of severity of the threats, and whether they perceive themselves as capable of protecting themselves. However, these theories focus on avoiding the involvement in information exchange and do not explain the decisions to share information, driven for example by the benefits of information sharing or trust in recipients' intentions.

Finally, Privacy Calculus approach [38, 39] is based on the premise that users reason rationally when deciding whether to share their data, in that they evaluate the costs and benefits of sharing their data and decide accordingly. This approach does not consider the impact of emotions, irrational behavior, information asymmetry, or lack of transparency that hinder the informed decision making.

In this section we have demonstrated that empirical evidence consistently finds information sharing preferences to be heavily dependent on contexts. However, theoretical attempts at defining such contexts and explaining the relationship between contextual factors and information-sharing decisions are fragmented and limited in scope. As privacy regulations and design of privacy-protecting technological solutions depends on understanding of users' information sharing behaviors, expectations and preferences in the context, there is an urgent need in comprehensive modeling of such contexts. Our study begins to address this relevant and important need.

3 METHODOLOGY

To study older adults' perspectives on information sharing, we conducted 1–1.5 hour semi-structured in-person interviews, in which we discussed: (1) what information they expect and do not expect various devices (including emerging technologies) to collect about them, (2) about collection and sharing of what information they feel comfortable or uncomfortable, (3) with whom they would be comfortable or uncomfortable sharing this information, and (4) how this information can be used or misused.[1]

We reached out to inhabitants of nursing homes and senior residences, members of senior centers, and cultural organizations for retired people in the San Francisco Bay Area. We screened potential participants using surveys in several formats—online, phone, paper, and in person—but excluded individuals with serious cognitive impairments and non-English speakers. With IRB approval, we conducted interviews in May and June 2018 with 46 participants at locations of their choice: private residences or public senior centers, and paid $20 as compensation. At the end of the interviews, we administered exit surveys about participants' individual characteristics.

Analysis. We audio recorded the interviews and had them professionally transcribed. Three researchers independently developed the initial codebooks using open coding. The initial codebooks were discussed and merged, and disagreements were jointly resolved. Four researchers used this codebook to code the rest of transcripts (two researchers per transcript), and to re-code the transcripts used for initial codebook development. Other results from this data set have been previously reported [49].

For the scope of this paper, we focused on a subset of codes related to information-sharing decision making (such as "ok to share," "not ok to share," "it depends" and "I don't know"). Two researchers applied thematic analysis to the excerpts identified under this subset of codes to further construct a list of factors affecting such decisions, until they reached saturation.

[1] In addition, we explored privacy- and security-related concerns and threats, user management strategies, and general opinions of older adults on emerging technologies in relation to daily needs and difficulties. Threat models, concerns, and mitigation strategies are presented in [49]. The interview guide can be accessed at https://tinyurl.com/interview-guide-seniors. Entry and exit survey instruments can be accessed at https://tinyurl.com/survey-seniors.

In iterative discussions, the two researchers then sorted and clustered the factors identified in thematic analysis following an affinity diagram process. During that process, we made some observations about the apparent relationships between the factors. Due to the qualitative nature of the analysis, the relationships described in this paper do not reflect statistical correlations, but rather conceptual connections between the identified themes.

Because the main purpose of this strand of our research is to identify factors that may affect information-sharing decision making, and not to make assessments about the prevalence or relative impact of those factors (which is a subject of our future survey research), we do not attempt to reach quantified conclusions. Instead, in line with the widely recognized norms of qualitative research [15, 21, 118], to demonstrate the dependability of the findings, in addition to including a detailed description of the analytical procedures, we support the findings with abundant quotes.

Limitations. We conducted our study in an urban/suburban area with relatively good technology resources, programming, and services for older adults, and a relatively high average income due to the high cost of living. Our sample is therefore not fully representative, though it is diverse in terms of level of independence, health, living arrangements, and activity. Because we primarily recruited through senior centers, programs, and living facilities, which often offer computer classes, our participants may be more likely to have attended or at least heard about such classes, and therefore may have more awareness of privacy and security issues.

4 PARTICIPANT CHARACTERISTICS

Our 46 participants were 65–95 years old (mean=76), 65% female, mainly white (76%), with self-reported native or bilingual English proficiency (45%) or advanced non-native proficiency (37%). The majority have an advanced (44%) or Bachelor's (33%) degree, live alone (63%) in rented or owned accommodations (87%) (the rest live in senior care facilities), and do not have a caregiver (80%); 9% have a hired caregiver, 7% a informal caregiver, and 4% have both. Respondents self-reported "excellent" (17%), "good" (50%), "fair" (24%), "poor" (7%), and "very poor" (2%) health conditions. Income level is below $35K for 35%, $35-75K for 35%, $75-150K for 13%, and $150K+ for 9% of the participants (9% did not specify).

Device Type	Daily	Sometimes	Never	Daily Out of Users
Mobile phone or smartphone	52%	22%	26%	71%
Tablet	22%	24%	54%	48%
Computer/laptop	61%	22%	17%	74%
All three	11%	39%	–	28%

Table 1. Device use among participants.

Table 1 shows how frequently participants use common devices: mobile phones or smartphones, laptops or computers, and tablets. The percentage of our participants that use all three, 39%, is similar to the figure for the general adult US population, 36% [11]. Just 11% of the participants do not use any of those devices.

To further assess participants' experience with technology, we asked in the exit survey how difficult it is for them to perform certain tasks using digital devices; the results are summarized in Figure 1.[2] Most of those who tried performing basic tasks felt fairly confident doing so, but relatively small percentages of our participants even tried to perform more advanced tasks.

[2] One participant did not respond to the question.

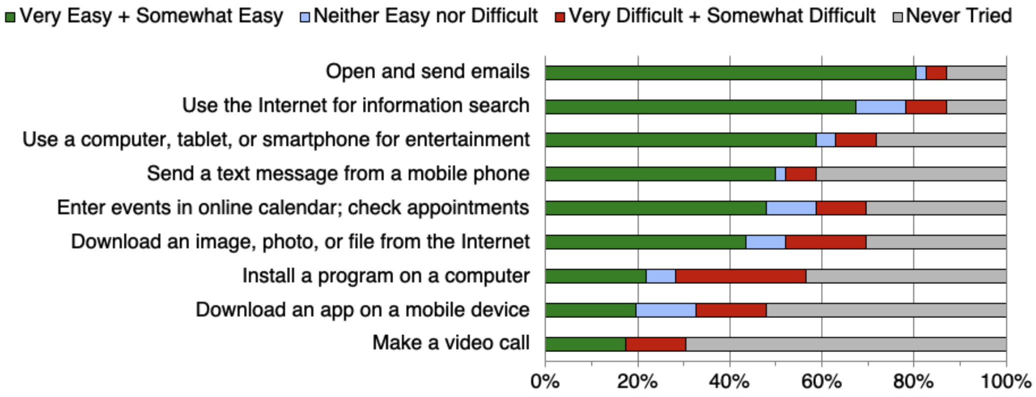


Fig. 1. Participants' facility at performing online tasks.

5 HIGH-LEVEL FINDINGS

In this section, we present some high-level findings about common information-sharing scenarios.

5.1 Opinions Are Context-Dependent

Interview respondents expressed a wide range of opinions about what data-sharing practices they find acceptable, along with perceptions and self-reported behaviors. Prior to asking about recipients and about use and misuse cases, we asked participants about what information they would feel comfortable or uncomfortable sharing. In response, they often not only talked about data types *per se*, but described whole scenarios of information collection, sharing, storage, and use, specifying the recipient, the purpose for information transfer, or other conditions that they believe would drive their decision in a specific situation. Sometimes the same participant expressed opposite opinions about their willingness to share a certain piece of data, depending on the context. This supports the idea, common in the research literature, that information sharing preferences and beliefs are contextual [e.g., 2, 12, 58, 66, 76, 85, 87, 88, 90].

5.2 Paradigm Examples

While some participants described detailed scenarios and conditions for information sharing, others used paradigm examples as shortcuts in expressing their sharing preferences. For example, medical and financial information were often used as paradigm examples of potentially-private information, and doctors and family as paradigm examples of benevolent recipients, while strangers were paradigm examples of unfavorable recipients. In such examples, one element of information flow (usually information topic, or recipient) was often used to evoke a whole sharing situation, while other elements (e.g., purposes of information sharing or use, benefits, and risks) were implied (see §5.2.2). Using thematic analysis, we explored common patterns in participants' views and identified several scenarios that were common in our data.

5.2.1 Views on sensitive data types. Respondents were usually unwilling to share financial data (either credentials or information about assets) and medical records. In the rare examples when participants said that they would accept sharing such data, it was usually in the context of very trusted relationships, and was used as an illustration of that trust:

> I would not want anyone other than our son knowing financial information about us. (P123)

In contrast, several people were against the prevailing concern about medical information sharing because they believe such sharing increases the chances of learning about, providing, or receiving better care:

> As far as medical records, I am not even that concerned on, the privacy to me seems like overkill. The concern about the hoops I have to jump through to be able to order the wife's prescription or to speak for her. (P123)

Interestingly, while phone number and physical address were often considered sensitive personal contact details, few participants mentioned that the email address is a valuable piece of information. This may be related to the fact that threat models involving abuse of phone and address information are more available to older adults, who often reported concerns or even experiences with telemarketing, robocalls, and risks of physical harm and burglary. Email marketing may be also perceived as less annoying, intrusive, or dangerous compared to robocalls. The most common (and almost only) risk associated with sharing email address mentioned by our participants was email spamming. Only a few respondents were concerned about email scams or about hacking or unauthorised access to their email, and no one mentioned the security risks associated with using an email account for resetting credentials for other potentially-sensitive accounts, such as online banking, shopping websites with stored credit card information, or patient portals.

5.2.2 Recipients and purpose of use. When talking about recipients, respondents often implied a combination of *who* receives the data and *what* they are going to do with it (cf. [6, 14, 88]). For instance, respondents often referred to sharing with "doctors" or "medical professionals," which implicates certain purposes tied to that role (diagnostics, tracking medical conditions, etc.). On the other hand, participants might refer collectively to "hackers" or "attackers," implying their obvious malicious intention to misuse personal data.

In addition to obviously and intentionally malicious actors, such as hackers, participants often expressed concerns about strangers and unknown recipients, and companies obtaining the data without explicit consent, and using it to the data subject's detriment (e.g., using online browsing and search data for unsolicited marketing or targeted advertising).

Our respondents were commonly willing (or at least not opposed) to share the data, even data they viewed as sensitive, such as medical records, or location, as long as they expect the recipients and the purposes of collection to be benevolent. They often mentioned benevolent recipients that include medical staff and close connections (family, friends). Sometimes respondents did not oppose sharing the data with the system developers and device manufacturers under the condition that the purpose of use will be limited to the provision of a primary functionality of such system/device.

The benevolent purposes usually imply benefits for the data subject, others, or to society as a whole (e.g., through research, proliferation of best practices, or analysis of trends and correlations). Among personal benefits, the largest group was related to ensuring safety and healthcare (including health monitoring and assistance in emergency situations), followed by more general assistance, such as providing recommendations, enabling home control, or assisting in navigation.

5.3 Disentangling Contextual Factors in Paradigm Examples

Some researchers focus on paradigm examples when examining information sharing attitudes or behaviors. Such studies try to identify what information types and topics are more sensitive than others [e.g., 95], or to quantify the value of privacy [e.g., 2]. In our data, while paradigm examples were common shortcuts that participants used to express their willingness or unwillingness to share information, the judgments of those examples were not unanimous among our participants. Some people were not willing to share certain information even with their family or friends:

> I'm in the closet, a bisexual guy. I don't really want to let the world know, even my immediate family. I go to like bath houses and I like transsexual people. (P9)

Others did not object to public sharing of their medical or location data:

> I would not be concerned that anyone here in the building would have access to my medical records. I don't see it being so private. (P123)
>
> *[Interviewer: Is there anyone you wouldn't want to know where you are?]* No, I don't think so. (P6)

In those cases, choices were typically determined by specific aspects of the situation (including participants' personal attitudes), rather than norms or typical behaviors of others.

Moreover, the prevailing answer among our participants about whether they would or would not share certain data was "it depends." For example, location, physical activity level, sleep patterns, and communication history and content (as data types), companies (as recipients of the data), and targeting of recommendations (as purposes of use) elicited equivocal and idiosyncratic opinions and were not unanimously perceived as appropriate or inappropriate data types, recipients, and purposes. Instead, the opinions of respondents about those categories of data sharing were highly heterogeneous, often with opposite valence, and often depended on complex trade-offs.

These fine-grained and diverse opinions motivated our attempt to unveil the implicit factors affecting the formation of both paradigm examples, and nuanced individual preferences on information sharing. While previous research has explored some of the elements of information sharing attitudes, in our opinion this topic still lacks a comprehensive and systematic representation.

6 MODEL OF DECISION-MAKING FACTORS

After conducting thematic analysis of the interview data, we focused on the elements of the data-sharing process, including conditional and contextual factors that participants mentioned in their answers about data-sharing preferences and behaviors. We used an affinity diagram process to group these elements and analyze the relationships between them (with reference to previous literature where relevant). As a result, we built the information-sharing decision-making model, which we describe in detail in this section.

The model is organized as follows:

1. At the highest level, the factors we identified are grouped into **dimensions** of information-sharing transactions, for example *data*, *recipients*, or *risks* associated with sharing.
2. At the next level, we identify the **factors** within each dimension. Factors distill the observed themes in what participants told us had affected their past sharing decisions and reactions to sharing events, or might affect hypothetical sharing decisions or reactions in scenarios we asked about, for example *trust in a certain recipient*, or *the likelihood of a particular negative consequence occurring*.
3. At lower levels, we identify the **sub-factors** and **sub-sub-factors** that contribute to formation of a specific factor. For example, *past experiences within the relationship* (sub-sub-factor) contribute to *the decision maker's perception about the recipients' intentions*, and *recipients' perceived intentions* (sub-factor) contribute to *trust in that recipient* (factor).

Figure 2 provides an overview of the factors, organized into dimensions, and Appendix A provides a complete listing of dimensions, factors, sub-factors, etc.

The seven dimensions can be summarized as follows:

- The **Decision Maker** is an actor making the decision about whether to share certain information or not; she/he/they may or may not be same person as a data subject (see §6.2.6).
- **Data** is any information about the data subject.

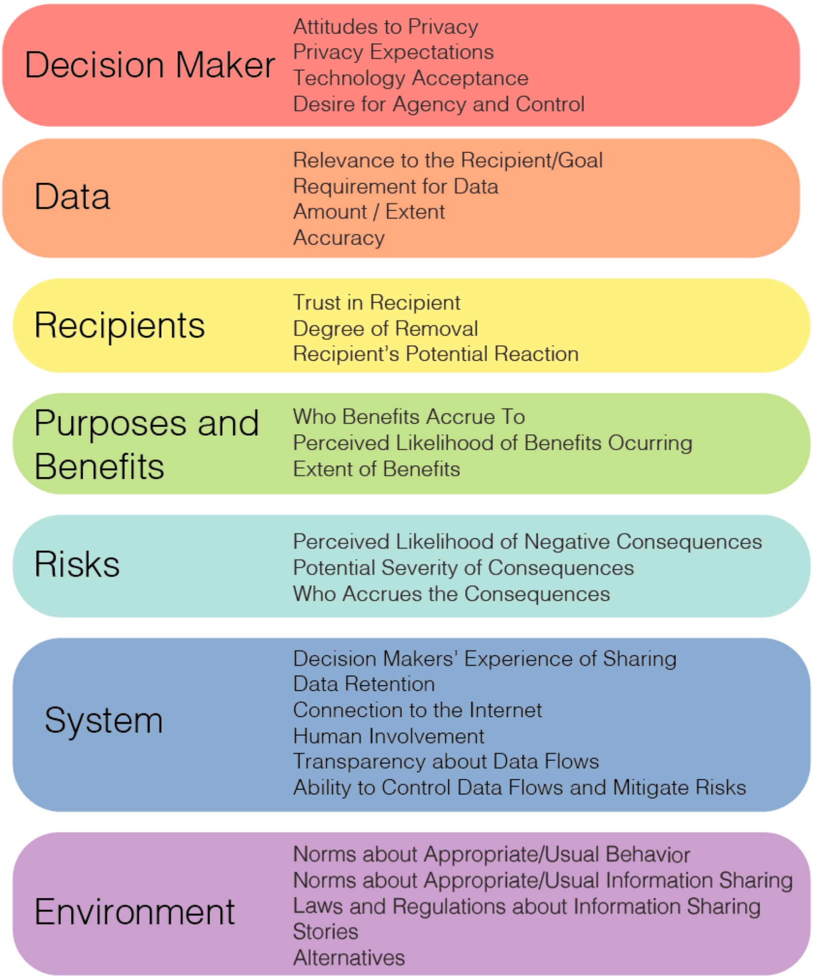

Decision Maker
Attitudes to Privacy
Privacy Expectations
Technology Acceptance
Desire for Agency and Control
Data
Relevance to the Recipient/Goal
Requirement for Data
Amount / Extent
Accuracy
Recipients
Trust in Recipient
Degree of Removal
Recipient's Potential Reaction
Purposes and Benefits
Who Benefits Accrue To
Perceived Likelihood of Benefits Ocurring
Extent of Benefits
Risks
Perceived Likelihood of Negative Consequences
Potential Severity of Consequences
Who Accrues the Consequences
System
Decision Makers' Experience of Sharing
Data Retention
Connection to the Internet
Human Involvement
Transparency about Data Flows
Ability to Control Data Flows and Mitigate Risks
Environment
Norms about Appropriate/Usual Behavior
Norms about Appropriate/Usual Information Sharing
Laws and Regulations about Information Sharing
Stories
Alternatives

Fig. 2. The proposed qualitative model of contextual information-sharing decision-making.

- **Recipient** is anyone—individual, group of people, or company/organisation—who has access to the Data (including the computer systems belonging to a company).
- The next two dimensions—**Purposes and Benefits** and **Risks**—are related to the use of information, which some models describe as 'purpose.' The purpose of data collection and use may be beneficial or detrimental to the data subject or decision maker. It may also be beneficial for some stakeholders and detrimental to others, depending on their goals. Even when the purpose is not intentionally malicious, it still may pose risks (e.g., due to a data breach or uses that the decision maker ends up feeling uncomfortable about). Moreover, the trade-off between benefits and risks has been repeatedly shown as the fundamental principle of information disclosure decision-making [31, 49, 106, 117], and is the foundation of the Privacy Calculus [39]. Therefore, in our model, instead of including the purpose of data collection/use as a single dimension, we consider separately the Benefits and Risks that collection, storage, sharing, or use of Data may imply.

- The **System** is an operational mechanism (usually a technological instrument, channel or infrastructure, such as a device, mobile or web application, platform, or other software) for collection, transfer, storage, and manipulation or analysis of the Data.
- **Environment** includes the exogenous contextual circumstances of the data-sharing scenario (outside of the System), such as sociocultural norms or news stories, that can affect decisions.

The flow of the model (see Figure 2) can be thought of as follows: (1) a Decision Maker decides whether to share (2) certain Data with (3) the Recipient(s), who may use it for (4) some particular purpose(s) that may incur some Benefit(s) and (5) may carry some Risks, (6) via a particular System (7) in a given Environment.

Each dimension is described in a subsection within §6, and each factor in a subsubsection. To help navigate the model, you will see color-coded boxes:

- The factors in each dimension are listed in boxes with *solid-color* backgrounds, at the beginning of the subsection for that dimension.

- If a factor has contributing sub-factors (and sub-sub-factors), they are listed in boxes with *white* background and color outline, at the beginning of the subsubsection for that factor.
- *Sub-factors described under other dimensions/factors, but contributing to the factor under question, are in italics and give a reference to the subsection where they are described.*

Caveats. The model has a few caveats:

- The dimensions are analytical artifacts aiming at systematic presentation of the elements in information-sharing scenarios; our decisions about how to group the factors into dimensions do not have consequences for the predictions of the model. As we noted in §2.2, our decision of factor organization along the chosen dimensions is in part driven by what could be most useful for designing and evaluating systems. For example, we separate out factors lying outside the system (the Environment) from the System itself, as both designers/developers and users have more direct control over the latter.
- While the order in which we present the dimensions is a logical flow of information *post facto*, it should not be understood as an assertion about the order of the decision maker's thought process.
- Identified lists of factors, contributing sub-factors, and options represent the themes we identified in our data, but are not intended to be exhaustive.
- Not all participants explicitly acknowledged every dimension and factor, or described the dimensions in isolation.
- No inherent valence should be assumed for any factor in this model: any of the factors may inhibit or encourage willingness to share in a given situation, depending on the individual effects, contextual factors, and particular interactions between factors in that situation.
- The relationships between factors and sub-factors play an essential role. In addition to the descriptions of how sub-factors may *contribute to* factors (or to other sub-factors), we will discuss other types of relationships and trade-offs between factors and sub-factors at the end of each subsection where appropriate (marked by the symbol ⇆).
- A factor should *not* be interpreted as being comprehensively described by its contributing sub-factors. For example, a decision can be attributed to a decision maker's *privacy attitudes* without any reference to what sub-factors contributed to the formation of that attitude.

- Participants often based their judgments (or past decisions they described) on expectations and assumptions—for example, about who will be the likely recipients of data—rather than on specific knowledge. However, the absence of evidence for their assumptions does not undermine the predictive possibilities of the model, as long as participants believe their expectations and assumptions are true or at least likely.
- We did not explicitly model participants' awareness or lack thereof about given elements of the information transactions, under the premise that the elements that a particular decision maker does not know about do not affect their decision.
- While our questions were usually about information transactions involving technological means, sometimes participants used examples from offline interpersonal communications as reference points while they deliberated over their answer to an online-sharing question. Whether or not they said in the end that their decisions would be the same in the two contexts, it is clear that attitudes about offline sharing can influence attitudes and behaviors in ICT-enabled information exchange. We therefore included those offline scenarios in developing the model.

6.1 Decision Maker Dimension

Factors in the **Decision Maker** dimension:

- Attitudes towards privacy
- Privacy expectations
- Technology acceptance
- Desire for agency and control

The decision maker in our model is a person who is making the decision about whether to share a certain piece of information. The Decision Maker dimension describes what characteristics of that person may affect her decisions. Note that these characteristics are based on participants' self-reported opinions, and do not necessarily align with the actual sharing decisions.

6.1.1 Attitudes to privacy.

Decision Maker > Attitudes towards privacy

Sub-factors contributing to this factor:

- Circumstances that make the decision maker feel especially vulnerable to certain risks
- Personal experiences with privacy or security violations
- *Decision Maker > Privacy expectations (§6.1.2)*
- *Environment > Norms about appropriate or usual information sharing in a given context (§6.7.2)*

Attitudes toward privacy comprise individual opinions and beliefs about one's personal information, and general willingness to share it. For example, one of our participants describes it as follows:

> Some people open to talk about anything, other people are not. [...] It's up to an individual's discretion as to [...] what boundary they have for their privacy. I guess there's no blanket guideline as to what people should or should not do. (P37)

Such attitudes can affect sharing choices:

> *[I: Who should not have access to this information? [...]]* Strangers. People that shouldn't have it—like, it's not the government's business. It's not any church's business. [...] It's not [the senior center's] business. I guess you could put the whole thing into 'others.' [...] it's my stuff, it's my business. I choose who I share it with. (P22)

In addition to general attitudes, some participants cited attitudes specific to particular data types:

> Well, my finances are really nobody's business. That is taboo. [...] My spiritual beliefs, my religion if there is one. [...] Again, it's a private thing. Essentially, my health. (P22)

Circumstances that may make a decision maker feel especially vulnerable to certain risks include particular historical background, socioeconomic, financial, or living situation, political, or religious beliefs, and sexual orientation (see more extensive discussion in Frik et al. 2019 [49]). These may cause decision makers to refrain from sharing personal information. Those aspects may affect the attitudes even when the the decision maker believes it is unlikely to actually face the associated risks any consequences. For instance, one participant in our interviews mentioned that although he feels safe today, the memories of historical events make him more privacy conscious:

> Jews don't face the repression in this country today that we faced in my parent's generation, okay? [...] So I am never completely far removed from thoughts of political repression. [...] I am not particularly concerned for myself now [...]. Nonetheless, I'm not ignorant of what's going on and what can go on. That's why I value privacy. (P113)

Some circumstances, for example specific health conditions or financial situation, also make people more vulnerable to certain risks, and trigger privacy concerns and increased perception of sensitivity of personal data:

> I'd be very careful about [my banking information], because [...] I live on a limited income, and that's all I need to get robbed, or something. (P10)

On the other side of the spectrum, people who believe that no particular circumstances make them especially vulnerable to certain risks, may feel less concerned about their privacy. The particularly common example is when people believe that they have "nothing to hide," and their lives are uninteresting enough to not worry about personal information disclosure:

> I lead a very boring life. There isn't anything that I can think of that I'm doing that I wouldn't want anybody to know. (P43)

> My life is an open book [...] I don't mind if people know any of these things I have done or that I have been through or that I have been involved with. (P35)

Personal experiences with privacy or security violations can also affect a decision maker's privacy attitudes. For example, after Participant P16 got scammed, he became more cautious about sharing information:

> So I have now [...]I tell my friends, don't do any information out, but best, if you interested in that, just call me, send the letter for me. I can check that. I think that this is the best way. (P16)

Past experiences with violations do not necessarily increase concern. For example, when we asked P35 whether sharing some personal information would bother her, she answered:

> Not really. I've been in Big Brother situations where I was politically active in late Sixties. (P35)

In other words, her prior experience as a political activist in the context of government surveillance desensitized her attitudes to privacy.

⇆ Connections and Trade-Offs ⇆

Specific to the elderly population, participants living in a senior living facility often mentioned an attitude of resignation about privacy. They may be willing to sacrifice some privacy in exchange for *Benefits* such as institutional care or better health outcomes—or, on the other hand, for continued independence:

> You cede a lot of your personal privacy rights when you move into a place like this, in exchange for services being rendered to you. So I think that's a different kind of a setting than somebody that is living in a private setting and would be using devices. (P71)
>
> I would probably chose [to share data on my] presence over having to share a room with somebody being in a nursing home. So if I could stay in my own abode [...] that is a concession that I would make. (P24)

6.1.2 Privacy expectations.

Decision Maker > Privacy expectations

Sub-factors contributing to this factor:

- Decision maker's perception of their own ability to understand the data sharing scenario and potential consequences
  - Knowledge of the specific data flows and mechanisms involved
  - Past experiences with similar or related data sharing scenarios (including benefits and risks)
- *Environment > Norms about appropriate or usual behavior in a given context (§6.7.1)*
- *Environment > Norms about appropriate or usual information sharing in a given context (§6.7.2)*
- *Environment > Laws and regulations about information sharing (§6.7.3)*
- *Environment > Stories (§6.7.4)*

Privacy expectations reflect a decision maker's understandings of the prospects of data sharing, i.e. what is likely to happen with the shared information, when it is likely to be (re)shared, with whom, why, and how.

In particular, the decision maker's ***perception of their own ability to understand the data sharing scenario and predict the potential consequences*** (including benefits and risks)—i.e. their self-assessment of whether their expectations are likely to be correct—may affect their decision about whether or not to share some data:

> I don't use a wireless backup, a cloud back up. [...] The sharing just surprises me sometimes. Phew. You don't know how stuff can go from one to the other, you are surprised it's there. (P123)

This self-assessment of understanding may rely in part on the decision maker's *past experience with similar scenarios*:

> The two times that [identity theft] has happened to us, routine controls would stop those things from happening. [...] There is hardly any defense against a dishonest person that can pull credit bureaus selling good bureaus' information. And you never read anything about that possibility. That's what had to happen on the credit cards that hadn't even been used in two or three years. Anyway we know to close accounts you don't use. (P123)

Participants may also take stock of their *knowledge about the specific data flows and mechanisms* pertaining to the situation under question. Such knowledge often relies on analogies with more familiar technologies (cf. [83]), for example, when the decision maker form expectations about mobile Internet browsing on prior experience with web browsing on a computer, or expectations about the data practices of a smart speaker (e.g. Alexa) based on prior knowledge about the data practices of mobile voice assistants (e.g. Siri). We identified that some of those expectations are correct, others are not:

> It's actually possible that when you are looking at Cable TV they could look at you back. You know. I suppose [for] a smart TV it would be even easier. (P25)

> Nothing much has changed. The format for collecting data like this has changed, it's a lot easier now because it's all computerized and collected automatically. Before it had to be collected by telephone, focus groups, somebody sending information back, complaints to improve products. But now, it's the products themselves, [...] they're constantly monitoring their own performance. (P71)

Privacy expectations may also depend in part on other factors in the model, such as sociocultural *norms about appropriate information sharing* (§6.7.2):

> I would be concerned about [video recording], inside the home. Outside, I would not be concerned. I don't feel like I've got an expectation of privacy when I'm out. [...] I do have an expectation of privacy when I'm in. (P15).

⇆ Connections and Trade-Offs ⇆

A decision maker may have *privacy expectations* relating to the factors of any other dimension of the model (other than Decision Maker). For example, the difference between a decision based on *data retention* and a decision based on *privacy expecations* about *data retention* is in whether the decision makers believe themselves to have concrete knowledge about a system's data retention policies or whether they are making an assumption based on their perception of what such systems usually do, whether the provider is taking advantage of their data, etc.

A Decision Maker's privacy expectations can be supported by improved *transparency about data flows* (§6.6.5); participants mentioned not being confident in their expectations due to not having sufficient information:

> Having not purchased these things, I don't know who they give the information to, you know, where it goes when you buy it. [...] I don't know what all that means, so I don't want to agree to something until I know what it means, you know? (P34)

6.1.3 Technology acceptance.

Decision Maker > Technology acceptance

Sub-factors contributing to this factor:

- Technology self-efficacy
  – *Decision Maker > Privacy expectations > Understanding of the sharing scenario (§6.1.2)*
- Circumstances that increase the need to share certain information

A decision maker's degree of **technology acceptance** can also be described as their general attitudes towards using technology to share information. Some people have a rather favorable attitude and appreciate the convenience[3] and speed of information sharing over electronic channels:

[3] Convenience and usability, measured as effort and time required to use a particular functionality, affect many of the dimensions' factors in our model, such as the degree of technology acceptance in general (§6.1.3), and acceptance of Internet-enabled transmission channels particularly (§6.6.3), decision maker's experience of sharing their data (§6.6.1), ability to control data flows, mitigate and protect against the risks (§6.6.6). Since the manifestation and impact of convenience and usability on these aspects slightly differ, we will discuss them separately in the respective sections.

> I [have] good doctors that allow me to work with them by e-[mail]. I don't go to see them, I just email and we adjust medications. (P71)
>
> I really like being in [this particular health provider] because it is a closed system. They have all my data about my health. My prescriptions. My parents had real problems before it went electronic, their medical records. Because things they were taking actually didn't work well together and could cause problems. (P24)

Others are concerned about technology performance (see also §6.2.4):

> Can [the fall detector] tell who is going to fall, whether it's me or my wife? What about the pussy cat? The pussy cat jumps around. (P113)

or about the negative impact of reliance on ICT-enabled communication as compared to in-person human communication:

> Companionship—I think it's ridiculous. [...] I think companionship has to be the real thing. Even an animal is better than Siri. (P43)

Technology self-efficacy is the decision maker's belief that they can successfully use the technology, and make informed decisions about it. Among our elderly interviewees, many did not believe in their ability to understand, make informed choices about, and correctly use technology, which often negatively affected their willingness to collect or share information using electronic channels:

> I'm computer illiterate. [...] I don't know much about it. [...] I do have an email address, but I very seldom use it, and I don't use it enough, so that things are always happening to it and I don't know what's happening. (44)

Participant 46 specifically acknowledged difficulties with understanding the language used in modern user interfaces:

> That is a big thing with seniors. [...] The language that [system designers] use and the way they assume you know what it means, and a lot of times we don't, because we weren't, we didn't grow up with the computers. (P46)

Certain ***circumstances may increase the need for collection and sharing*** of certain personal information, which can also affect acceptance of the technology that collects it. For example, a decision maker in precarious health would have a greater need to collect and share vital signs:

> Given my situation, my health, [wearable fitness tracker] is something that isn't high on my list. [...] I know people who wear various kinds of monitors. Generally those wearables are worn because of a specific reason. They are subject to high blood pressure, they are subject to pulse fluctuating wildly and so forth. (P121)
>
> If you were, you know, frail and somewhat immobile, I think those little care robots would be great. (P22)

Similarly, an elderly person living alone will have a higher need to collect and share such information than a person whose vital signals can be regularly monitored by other household members:

> If we fall and are not movable, [...] we are basically depending on the other person to be able to pull the cord or something. [...] And then there is a number of people around here that have a pendant [alert button]. [...] I don't know if we will ever get them. As long as there is two of us, we probably won't get them. (P123)

⇆ Connections and Trade-Offs ⇆

Acceptance of technology interacts with the *Purposes and Benefits* of sharing (§6.4), and especially with the *extent of the benefits* to them (§6.4.3):

> *[I: Presence [data], it's kind of like if you walk into a room, the lights turn on like that. [...]]* I don't think that's necessary. Turn on the lights, or leave some lights on, which you should do anyway if you leave. (P5)

This interaction with the *extent of the benefits* is especially relevant in the Decision Maker's evaluation of whether their *circumstances increase the need for collection and sharing*:

> Am I harming myself by not taking advantage of all this stuff? Am I limiting my life? [...] Part of me thinks, how many years can I just continue to live my little simple life? Maybe I won't live that long and so I'll never have to get into [...] learning to use all of these things, because I don't really need them. [...] People always express surprise that I don't really have a digital life, but my answer to that is, 'You know what, I'm sixty-five and I am getting along pretty well without all that right now, so maybe I don't really need to. Maybe I can just sort of keep life simple.' And then, be just more anonymous, more protected, more private, which is just sort of the person I am. (P47)

Acceptance of technology may interact in a specific situation with the perceived *Risks* of sharing (§6.5) in that situation, i.e. the *perceived likelihood* (§6.5.1) and *perceived severity of potential negative consequences* (§6.5.2), as balanced against the *extent of the benefits* (§6.4.3):

> If I look it up on the map, I know where I am, and the kids today don't know how to read a map, so they depend on their GPS. [...] *[I: And you don't want to share your location?]* No. [...] You can put in your address and you can find exactly on, you know, the computer, exactly where you live, and I think that's an invasion of privacy. [...] For your own safety, I don't want that published all over, as where you can find me. (44)

6.1.4 Desire for agency and control.

Decision Maker > Desire for agency and control

Participants sometimes expressed their degree of **desire for agency and control** over personal information as a general individual trait:

> It's just because of where I came from and that was a very negative thing. [...] Actually if you ask me a question, I will probably just tell you. But the idea that somebody would know it without me telling them is different. It's different. In my world, that's huge. I should be the one that breaks the news, not an app. (P24)

> I guess I'm just a private person [...] Just, just having my own life. You know? Having some control over my private life. (P34)

Some other respondents framed agency and control as an attempt to exercise a fundamental right of ownership over one's personal data, manifestation of (or willingness to protect) independence:

> The one thing you lose as you get older is control, so you hold onto it. Even when you shouldn't at times. (P24)

> I don't really have very much to hide. [...] But, people have a right to privacy, have a right to be left alone and they certainly ought to have a right to draw limits to what others can do to them. (P113)

and a push back against the current not fully transparent data practices or not offering meaningful choice about them:

> I don't want anybody to have access to any information about me, unless I give it to him. [...] If I give my permission for somebody to have it, if I want to share it, then that's fine. They would have to ask me first. (P1)

A specific concern our participants often expressed is about who initiates the collection or sharing of information. For the most part, they are more comfortable when they actively initiate the data collection or sharing:

> I think about my psychologist who I've gone to for many many many years and he knows virtually everything, but I wouldn't want him to just open up something and have all of my medical records, and, yet, I tell him probably everything that would be in a medical record. [...] I want to be the informer. (P32)

Some people, however, have a weaker desire for control over their information, or do not feel empowered to keep it, and are more ready to let it go:

> Some things you have no control over and can't do anything about. [...] I want my information back and they say "no"—sometimes you just have to go ahead and okay. Sayonara, out the door. [...] I mean you can't–not everybody can fix everything. You just have to live with the consequences. (P107)

But even users who did not express a deep desire for control sometimes qualified those attitudes by pointing to other features of the context that might make them more willing to relinquish it:

> I don't really care. If a doctor told me to keep a record of [my sleep], I guess I would [use a wearable device]. (P110)

⇆ Connections and Trade-Offs ⇆

Attitudes about agency and control may or may not correlate with *privacy attitudes* or levels of concern (§6.1.1). One the one hand, a person concerned about their privacy may be more willing to monitor and control how and with whom their data is shared, and personally grant the permission. On the other hand, a privacy concerned individual may not have the desire to control personal data, for example, if they *trust the recipient* (see §6.3.1), or if they do not believe such control is practically feasible (§6.6.6). At the same time, a person with strong desire for agency and control, may not be comfortable sharing personal information, not necessarily due to specific privacy concerns, but due to discomfort associated with the loss of agency over one's private data.

6.2 Data Dimension

Factors in the **Data** dimension:

- Relevance to the recipient/goal
- Requirement for data
- Amount/extent
- Accuracy

The Data dimension describes the particular characteristics pertinent to a specific piece of data (e.g. how many miles the decision maker walked on March 3) or to a category of data (e.g. daily exercise levels) that may affect participants' decisions to share it.

As we noted in §5, some theoretical models and empirical studies focus on *categories* of data—"data types" or topics (such as medical, financial, demographic, contact information)—rather than on *characteristics* of that data. However, despite attempts to categorize information into sensitive and not sensitive, perceived value and preferences about which would be shared by all users, research on privacy consistently finds evidence of idiosyncrasy and context-dependency of privacy preferences, expectations, and behaviors [12, 17, 76, 85, 87, 88].

Some of our interview questions were in fact phrased in terms of data types or topics, and participants often referenced such categories as paradigm examples (see §5). In some cases, participants stated that particular data types are considered sensitive or private, without further explanation

> I just wouldn't want anybody to get into my medical records. I mean, that's personal, you know, personal information that is mine. I don't want everybody to know it. (P14)

However, in the same vein as the research mentioned above, we believe these paradigm examples and gestalt judgments are in reality a product of the interplay of several different factors, which may be restricted to certain prototypical sharing scenarios. Because the interviews were semi-structured, we were able to probe for details about why participants might view data as sensitive or not sensitive—especially for data types where there is less broad agreement about whether it should be shared in different situations. In particular, participants sometimes highlighted exceptions in their decision-making that occurred when a particular piece of data had a characteristic that did not match the usual for that data type, or where their views differed depending on the specific piece of data involved:

> Location—I don't like somebody, some stranger to know where I live. [...] *[I: What about your specific location right now? Do you feel like that is also private?]* No, I think [the senior center] is OK. (P13)

In our analysis, we therefore aimed to dissect participants' explanations of their decisions (where they offered them), in order to identify the particular characteristics or situational dependencies that make those data types or topics more or less likely to be shareable or sensitive. Some of those characteristics are described in this section, while others are categorized as belonging elsewhere in the model, as we explain in §6.2.5.

6.2.1 Relevance to the recipient/goal.

Data > Relevance to the recipient/goal

Many participants explained their sharing decisions in terms of **relevance to the recipient/goal**, i.e. whether they thought the data would be useful or actionable for a given recipient in fulfilling the decision maker's goals and/or incurring a benefit. This line of reasoning was applied to explain the decisions to share:

> I am totally comfortable if that information [about appliance use or door states] is going to the people or the company or organization [...] that is monitoring these devices, to determine if someone is in some kind of danger. That is perfectly reasonable, if they know if I've left my doors open, or if I failed to close my door, or if I did something that is unsafe, like if I get too hot or something like that. (P47)

and not to share because they did not believe it would be useful towards achieving any benefit:

> I wouldn't be unwilling to give it to them but I don't think they would need it or use it. (P20)

The latter was often expressed as a doubt that anyone would even be interested (see also §6.3.3). In other cases, they did not want to share data because they were concerned that it *would* be actionable for the recipient—but not towards fulfilling the decision maker's goals:

> The only thing [...] that I would be eager to share is the medical information, because anybody who has a right to know it, needs to know it. As to the other [types of information], it is really nobody else's business and I do take my privacy seriously. [...] I don't want to be bothered by people trying to sell me something. (P113)

From this perspective, participants' evaluation of whether the data is relevant to achieving their goals depended, in large part, on their evaluation of whether the recipient's purpose in collecting the data is beneficial (see §6.4), and aligned with the decision maker's purpose in providing that data (see §6.3.1).

In most cases, participants spoke in terms of the data's actionability in benefitting themselves:

> If my doctor saw how little activity I have, they would probably intervene and tell me [...] I wouldn't mind. (P18)

But sometimes participants also talked in terms of data's relevance to benefiting ratified others:

> I would be okay sharing information with anybody who could put what happens to me to good use for how it might be beneficial to other people [...] for some reason that was important to whatever, education, learning, helping other people. (P35)
>
> If I felt that I could be a study and help to somebody for science or something, I would do it. I wouldn't care. For science. It's not going to help me! [...] I don't even consider that they would help me. It's too late. (P107)

6.2.2 Requirement for data.

Data > Requirement for data

Participants reasoned not only in terms of whether data *could* be used by the recipient to further the decision maker's goals, but also in terms of **whether that data is *necessary* to achieving the decision maker's goals**. In particular, their acceptance of data sharing often depended on whether this data is actually necessary for provision of a service or functioning of a device/app. Assuming they agree with the purpose of collection, participants generally said they are most likely to decide to share data when they believe it is an actual technical requirement for the system to function in general:

> I think [motion data is] absolutely necessary for home security. (P5)

or to function optimally:

> It'd probably have to know a lot about me [...] about a lot of my likes and dislikes. [...] Otherwise it wouldn't be a very good care robot. [...] At this point, I'm assuming I'd have to provide the information. (P24)

However, participants are aware that sometimes the system could achieve its purpose without the data being required, or with less data or a different type of data. Such requirements are often imposed arbitrarily by providers, as a condition of providing the app, device, service, or a particular functionality:

> I don't think they need to have a lot of other information that's just available, just because it happens to be available. And that's why a lot of these, like Facebook, and all of these entities collect a lot of information, [...] and then they're using it for other purposes. [...] So I think that the key for me, and sort of the laws that should regulate these things, how much of it is relevant, you know, to your specific need, and protects your privacy to the greatest extent under those circumstances. (P71)

6.2.3 Amount/extent.

Data > Amount/extent

Sub-factors contributing to this factor:

- Accumulation of data over time

  - Continuity of data collection
  - *System > Data retention policies (§6.6.2)*
- Granularity and specificity of the data
- The format of the data or the type of sensor

Some participants consider the **amount or extent of data that is collected** or could be collected. This might be phrased in terms of specific characteristics such as ***accumulation of data over time***. Accumulation may be an effect of *continuity of data collection*, i.e. whether it is ongoing or limited to a specific goal, as well as *data retention* policies (see §6.6.2). Generally, time-limited collection is preferred over ongoing monitoring:

> If someone came in and said, can we track you for a week because we are doing a nutrition study for people over eighty, I'd probably do it. [...] But ongoing, no. (P24)

Amount might also be considered in terms of the ***granularity and specificity of the data***:

> I have an advanced directive on my niece as my person. I keep her up to date on things, but she doesn't need to know my location every twenty-four hours a day or anything. (P71)

A few participants mentioned having different views on sharing depending on ***the format of the data or the type of sensor*** it is collected by, and their perceived invasiveness:

> Wall sensors [...] would have to collect atmosphere and noise. My mind would go, are they reporting this? If they have to listen to noise to know that I fell, how would they know? Is it sonic? If I trip it sends some kind of wave out that they pick up, or are they listening—Big Brother? (P24)

⇆ Connections and Trade-Offs ⇆

The *amount or extent of the data* was occasionally mentioned in isolation, as in the example above. However, amount, especially *accumulation over time*, usually came up in discussions about the *relevance of the data to the recipient/goal* (§6.2.1) and/or about the concrete *requirement for the data* (§6.2.2), in that a decision maker might view *some* data as being necessary and actionable, but not as much data as is being asked for:

> I would be comfortable sharing my location with people who might, like, respond to my need for assistance. [...] But I suppose I would also have[...] some concern that some people might be tracking me for some other purpose than to monitor my safety. [...] Why would anybody need to know where I, exactly where I was at all times, [...] if I am not having a problem? [...] Sharing it with somebody who just wants to try and sell me something then that's a whole other— a different layer of concern. (P47)

While usually considered more invasive and risky, ongoing data collection and accumulation may produce more *accurate* inferences and better achieve the purpose of collection (see §6.2.4). Other factors, such as *trust in the recipient* (§6.3.1), or *importance* and *urgency of the data collection purpose* (§6.4.3) may offset the negative aspects of ongoing monitoring. However, participants who mentioned data accumulation felt that the advantages and disadvantages should be carefully weighed, and data collection should be limited to a specific goal when possible:

> Will they get something from my pattern, what I– They would track my daily activities? [...] Save [...] what I'm doing every day so they can break into my house. I'm worried about that. So I don't want them to keep anything there. [...] If you cannot function at all, I need help, then I might sacrifice some of my privacy, but I just hope they can keep in the same place and it will not be hacked. (P103)

6.2.4 *Accuracy.*

Data > Accuracy

In making sharing decisions, some participants consider **whether data is likely to be accurate**. Among other concerns, sharing was seen as a potential source of inaccuracies:

> [Medical data] should be protected better. You wouldn't want somebody putting misinformation in your record. Or changing information in there, or something. Which could happen if a lot of people have access to your data that don't need to have access to it. (P71)

⇆ Connections and Trade-Offs ⇆

In some cases, participants brought up *accuracy* in terms of whether data would be *useful in achieving the ostensible purpose of sharing* (see §6.2.1) and thus how it affected the *likelihood* and *potential extent of the intended benefit* (§6.4.2, §6.4.3). For example, participant P121 views the collection of large amounts of information as having the potential for extensive benefit to medical science, but notes the importance of the base data being accurate and relevant:

> If one could relate [sleep patterns] to something else that is measurable, that would very well prevent long-term problems. A very very useful thing. [...] Certainly I would participate in a trial like that if [...] the aim were to find large scale understanding of what works. [...] So many of the gadgets that I hear about is solutions looking for a problem[...] But why should I be spending my time or my energy... [...] I mean, it is very, very hard to get dependable performance in old people, very hard. . (P121)

6.2.5 *A note on the relationship between Data and other dimensions.* ⇆

In addition to the characteristics described above, many of our questions about which types/pieces of data participants prefer not be shared garnered explanations that referred to characteristics we describe elsewhere in the model (i.e. other dimensions). Such explanation were framed with reference to that particular data type/topic or particular piece of information.

For example, many of the explanations of what makes a data type or piece of data sensitive were related to the *likelihood* (§6.5.1) and *severity of risks* (§6.5.2) should it become more widely known. In particular, sensitivity arising from risks could arise (or not) from the *potential reactions recipients might have* to the information (§6.3.3). Such descriptions often made reference to whether the data contained or implied information about violations of *social norms of behavior* or even *laws about behavior* (§6.7.1).

Particularly with paradigm examples such as medical or financial data, participants often make reference to *social norms about information sharing* (§6.7.2) that particular type of data, along with their own *privacy expectations* in that regard (§6.1.2). On the other hand, participants also drew connections between their own general *privacy attitudes* (§6.1.1) and their views on the sensitivity of particular data types or topics. In some cases, they highlighted tensions between their individual attitudes and general social norms about what types of data it is okay to share. For example, a participant might illustrate their generally open attitude by saying how easily they would share medical data:

> I don't see [medical records] being so private. I know it is. I know lawsuits are the reason, and so they have to be so, so, so, so careful. But I don't share that concern. It probably shows that I am naïve. (P123)

or, conversely, they might illustrate their very concerned attitudes about privacy by saying they would not share certain data even if it might not seem very sensitive:

> Nothing that I am keeping private is either illegal or immoral. It's mine. You know, it's my information, and in this age when we have so little privacy anymore, it becomes more precious. (P22)

Finally, participants might refer to the fact that some piece of data, or the information it implicates, is already widely known—in other words, defining whether it *should* be kept private in terms of whether it currently *is* kept private (§6.3.3).

6.2.6 A note on data subjects. In our interviews, respondents mostly commented on the decisions they would make about their own data (i.e. the same person is decision maker and data subject). We had few examples where participants considered situations where they were the decision maker and another person was the data subject. An exception was Participant P123, who helps his neighbors with computer problems:

> She didn't mind if I put [her] Amazon account in [my] phone, the credit cards and stuff, but I didn't want to get my Amazon account confused with hers, that's for sure. [...] I was concerned that, with Apple stuff, you don't know what shares. [...] Stuff can wind up on another computer so easy with an Apple. [...] I am cautious on that when it's somebody else's stuff. (P123)

In those few cases where participants did describe decision-making processes for other data subjects, we observed that, even if they tried to imagine what the data subject's preferences might be, they tended to project their own attitudes and preferences. And even where participants acknowledged that the data subject might have different preferences, they still might choose to behave as they would with their own data. For example, participant P110, a notary public, said:

> I think that privacy is important—in fact, often, when I meet [a client] they will say, 'The reason I want you to notarize this is I'm changing—I'm having my daughter become power of attorney,' or something like that. That's nothing anybody needs to know. So at least [in the facility library], they have the privacy and it's only between them and me. [...] *[I: It seems like your peers here seem to feel the need for some privacy around certain documents...?]* [...] They've never expressed that to me, but I would think that they might. I would. (P110)

Therefore, while some literature, including literature on Contextual Integrity [88], defines the identity of the data subject as an important parameter of data-sharing scenarios, we do not include *data subject* or *whether decision maker is the data subject* as a factor of our model. We are not by any means discounting the possibility that data subject may have an important effect on data-sharing decisions. However, because the goal of the study was to examine decision-making about one's own data, examples of decision-making for others were too limited to draw conclusions.

6.3 Recipients Dimension

Factors in the **Recipients** dimension:

- Trust in recipients
- Degree of removal
- Recipients' potential reaction

The Recipients dimension describes the entities or people who receive the information shared by the decision maker. Similar to the Data dimension, participants might refer to specific people or organizations they might or might not want to share data with, or might reason in terms of categories (e.g. daughter, friend, physician, salesman, hacker). However, such categories often do not carry a universal meaning, and rather represent an interplay of different factors affecting the decision making. For instance, the decision makers may say that generally they are comfortable sharing information with the family, but their actual decision is much more granular than that, and may depend on who the family member is, the relationship with him, etc. Therefore, as with Data, we did not analyze Recipients in terms of relationship "types" *per se*. Rather, we analyzed the characteristics of the recipients and the relationship with them that participants cited as important for their information sharing decisions.

6.3.1 Trust in recipient.

Recipients > Trust in recipient

Sub-factors contributing to this factor:

- Evaluation of recipients' legitimacy and (general) intentions
  - Past experiences within the relationship
  - Recipients' reputation
    - *Environment > Stories (§6.7.4)*
  - Assessment based on appearances
- Recipients' judgment and competence/ability

Trust in the recipient is the belief that the recipient will not use the information against the decision maker's best interests.

When talking about trust, our participants often used paradigm examples, usually describing the type and closeness of relationship. For instance, our participants typically expressed the most trust towards their families (with a variety of data types), and doctors (with a more narrow set of relevant information, such as medical records):

> My daughter knows absolutely all my email–or my, what are they? Passwords. (P107)
>
> *[I: The calendar and doctors' appointments and shopping needs and classes that you usually take? Who would you expect to have access to this information collected by this system?]* Just me. I mean if anybody, it would be my son. [...] Another person that might have access that I might be willing to have access would be my family doctor. *[I: Why?]* Well, just I would have no reason not–for him not to know all of this. You know, he might have some other recommendations based on what I'm doing or what I should be doing and might be helpful. [...] I'm willing to share it because I trust them and if they wanted it I would have no objection to giving it to them. (P20)

They trust strangers, marketers, or obviously malicious recipients, like hackers, the least:

> *[I: You mentioned also, that you don't buy things online because you didn't want to put your credit card number in. Can you talk more about why you don't want to do that.]* I just don't trust, there's so many hackers nowadays, that get into your computer. [...] They might hold of my cre– identity [...] and credit card, and take things out of my bank account . (P13)

However, relationships with a particular type of recipients are not always homogeneous, and as we mentioned earlier, opinions may diverge based on more specific characteristics. For example, in response to a question about whether she would be comfortable sharing medical information with family or friends, participant P47 answered:

> Certain ones. Yeah. The ones that I am on good terms with, you know. The ones that I trust, which is most everybody, you know. But it's theoretically possible there could

> be some family member out there who does not have my best interest in mind and then I think I would have to be hesitant because your medical information can be used for a variety of things. Like let's say somebody has got some kind of a legal proceeding, wants to put me in a bad light and they want to say 'This person [...] she's not competent to handle her own life. To make her own decisions. (P47)

Similarly, although most participants trust their doctors, they acknowledge that, albeit unlikely, such trust can be breached:

> I cannot think about the doctors as evil person. I just assumed they were good. The bad ones like that one Olympic gymnastic the doctor, It's evil. [...] He's the doctor you trust him, and he molest you in front of the parents. [...] most likely you don't think that way. Okay, when you go to see a doctor, you assume then they are good doctor. And most of them they are, right? Those are just bad apples. (P103)

Other types of relationship achieved even less consensus, such as friends, neighbours, government, and companies. Group identity was also sometimes used to describe the closeness of the relationship and therefore trust:

> I wouldn't tell anybody on the street down there. Talking about strangers, some guys at the bath houses I tell them, 'I'm [...] bisexual guy.' So I feel comfortable with that. *[I: Why do you feel comfortable with that?]* Because they are in my community. (P9)

> I suppose if somebody was radically opposed to my political thoughts I would probably be under the gun on that. (P25)

More generally, trust may be based on a decision maker's beliefs about a recipient's *legitimacy and generally good intentions* and their (*judgment and competence or ability*) to use data appropriately.

The ***evaluation of a recipient's legitimacy and whether they have (generally) good intentions*** relies on *past experiences within the relationship*, *the recipient's reputation*, and sometimes *an assessment based on appearances* (if the former two factors are not known). For example, some participants commented on ***past experiences within the relationship*** with their friends:

> I gave her my credit card number and everything. [...] This friendship is 40 years, and you know, there was no question about that. (P34)

or businesses:

> I do online banking with B of A [Bank of America]. I used to work for B of A for like 20 years. So I know their system's secure. (P104)

Regarding ***reputation***, participant P121 said that he would be comfortable sharing information if

> a reputable organization, which is well-managed, is collecting information. (P121)

When users are not familiar with the system, they have to rely on its ***appearance***:

> I try to avoid being involved in [other websites], which makes you think you might be a scam, like it's too good to be true sort of thing. (P110)

Even if the recipient has good intentions to handle data in the best interests of decision maker, a negative evaluation of the recipient's wisdom, i.e. ***judgment, or actual competence and ability*** to do it may undermine a decision maker's trust:

> Nowadays I think they send it to this security firm and they would have an employer, 24/7 monitor staff. I mean whereas if it is family monitoring, again, is [...] as good and as attentive as the person that is monitoring it; and people are emotional beings and they get distracted. (P37)

⇆ Connections and Trade-Offs ⇆

Going beyond references to generally good intentions, some participants frame discussions of trust specifically in terms of their degree of confidence in the alignment between their purpose for sharing the data and the recipient's primary in collecting and using that data. The relevant *purposes and benefits* (§6.4) may be defined broadly (e.g. improving the health conditions of the decision-maker), or specifically (e.g. medical testing to diagnose a particular condition). For some decision makers, the alignment with recipients' general (broad) good intentions is enough, as far as they benefit the decision maker. For others, the alignment of the specific purposes is important, e.g. the use of medical test results shared by the decision maker with a doctor for diagnostics, and not for sponsored recommendations of a medication, although both intentions aim at improving health. In the latter type of case, the recipients' purpose may be not explicitly malicious, but because of misalignment with decision maker's preferences, may still negatively affect the sharing decision:

> Well, the only thing I would share [information about my pacemaker] would be with another doctor, or with somebody in the healthcare industry. *[I: For example, who else in healthcare industry, except doctor?]* Oh, I don't know. I suppose some pharmaceutical company would be interested in that information, and then I would start getting ads for such and such medication. That's spam so who needs it.] (P25)

Trust is sometimes played off against the *relevance of data* (§6.2.1) at the same time as the *purpose(s) and benefit(s)* of use. For example, even a trusted friend might not be considered an appropriate recipient for information they could not usefully do anything with:

> I'd be willing to share [my medical record] with my doctor. But nobody else needs to know unless I'm dying or something and I guess I need to let my immediate family know. But total strangers or friends, even if they were close, I don't think it's their business. (P53)

Some participants drew connections between *trust in a recipient* and their perceptions about the recipient's *transparency* (§6.6.5) about the purposes and use for data collection:

> I would be uncomfortable if any of the data or applications that I use were used for business purposes, [...] to make money elsewhere. [...] To be taken advantage of. These devices are presented as though they are giving you new capabilities. But the capabilities could often result in somebody's abuse of your information. *[Later in the interview]* [Abuse is] if it were used in a way that was not totally transparent to the user. [...] If it were used for some other purpose that was not transparent to me. (P60)

6.3.2 Degree of removal.

Recipients > Degree of removal

The **degree of removal from the initial act of data collection/sharing** refers to how many consecutive intermediaries participated in the data sharing process between the decision maker and the recipient in question. For example, if the decision maker shares data with a service provider, the service provider is the primary recipient. A marketer who then receives the data from that service provider is a secondary recipient. If the marketer then shares the data with an insurance company, the insurance company is considered a tertiary recipient (from the point of view of the initial decision maker we are modeling), and so on. The more the recipient is removed from the decision maker, the less control the decision maker perceives themselves to have over the shared information:

> What happens when you go on to these other sites looking for something then you get a barrage of emails afterwards. And I either delete them and if they keep on coming I try to find the place I can unsubscribe to them. [...] It's mostly other companies that I never, I really never shopped in the first place that send me emails. [...] Those are the ones that I always want to get rid of. (P110)

However, it should be noted that answers to questions about potential recipients tended to center around people, and were often framed more or less as though the decision maker were considering what they'd share in person—even if the question was about using technology to share, and thus the person in question would actually be a secondary recipient.

6.3.3 Recipient's potential reaction.

Recipients > Recipient's potential reaction

Sub-factors contributing to this factor:

- Perceived desire to receive the information
- Expected affective reaction
  - Environment > Norms about appropriate or usual behavior (§6.7.1)
  - Environment > Norms about appropriate or usual information sharing (§6.7.2)
- Likelihood that the recipient already knows or could easily guess the information

When thinking about whether to share data, decision makers sometimes consider the **potential reaction of the recipient** to this information, including both their *perceptions about the recipient's desire to receive the information* and *expectations about their affective reaction.*

With regard to ***perceptions about the recipient's desire to receive the information***, participants often expressed reluctance to share data when they expected recipients not to be interested in it:

> *I: Did you share this journal with anyone, with doctor when you got to an appointment or anything? Like your weight or your blood pressure.* No. *I: Why not?* Why not? Nobody ever asked for it. I would tell them I kept a journal and I had this information, but nobody seemed particularly interested in it. (P60)

They also were reluctant to share the data when they expected a negative ***affective reaction*** from the recipients, such as worry, judgment, or disapproval:

> I believe part of the reason I value privacy so much is because there are people out there, fanatics, whether it's religious fanatics or political fanatics, who really cannot tolerate diversity, dissent. If they get on you, they can really make your– they can really mess up your life. (P113)
>
> When I initially had a tumor removed, [...] I did not tell [my family] until I had all the facts. [...] I didn't want to upset my father. (P36)

In contrast, some participants said that they would share the information to mitigate worry:

> I usually tell my sister if I'm going somewhere and she usually tells me if she has an appointment, or if she's not going to be home. So I think it's important, especially when you're older, because you never know what might happen. Or, what, like for instance, if she's going on a date, I think it's kind of important that she lets me know where she's going in case anything should happen. Especially when she goes on a date, that she met on her computer. (P14)

Judgments about data sharing can also depend on the perceived ***likelihood that the recipient already knows or could easily guess the information*** contained in the data, or whether that information would already be easily accessible to the recipient, for example because many people know it:

> *[I: For the activity and nutrition. Do you also feel that this is sensitive?]* What I eat? I think [my friends and family] know I'm pretty healthy. *[I: [...] And the activity?]* I don't mind knowing what I'm doing. [...] I'm usually here. I'm usually dancing, either here or at the senior center. (P13)
>
> *[I: And what kind of information you would be more comfortable sharing?]* Well, just about anything else. You know, where I got my jeans, how I feel about Donald Trump, thoughts I have about improvements to things, or things that I can improve in myself in a... You know, all things that are not, things that are out there already. (P22)

6.4 Purposes and Benefits Dimension

Factors in the **Purposes and benefits** dimension:

- Who benefits accrue to
- Perceived likelihood of benefits occurring
- Extent of benefits

Although the Purposes and Benefits of data collection may not always be known or explicitly communicated to the decision maker, they usually at least assume that the recipient has a purpose and that that purpose will benefit someone:[4]

> I would just assume that they are doing it altruistically. Okay? For good reason, for good purpose. (P107)

Many of our participants expressed the importance of knowing the purpose of data collection and use:

> I think I would always want to know, explicitly as to what the data is going to be used for, because what is the purpose in doing that if I would say Yes, but there is nothing about my life [...] that could be so acquired that it concerns me at all. In the hands of people who are trying to do a good job, no problem. (P121)

This includes concern with both the primary or ostensible purpose for data collection (usually what is explicitly offered to the decision maker, such as providing an online service) and with secondary purposes or uses (which may or may not be mentioned upfront, such as making money by targeting ads to customers), see §6.3.2.

We can categorise benefits discussed by our participants into three main domains: material, related to physical health or safety, and intangible. Material benefits include financial gain, for example from lower insurance rate, lower housing price or other subsidies (due to eligibility justified by the shared data):

> It could affect the cost of insurance or whether you could get a job. (P8)
>
> If I was younger, it might hinder me from jobs or even benefits of some kind. But [...] the only thing I can do now is to violate myself with the Section 8 site-based that I have for living in this residence and the SSI social security benefits if I were to go to work illegally or bring in more money than I was supposed to have, then I would lose my benefits. (P21)

[4] Unlike with Risks, the possibility that the recipient's purpose or use for data will result in unintended benefits was not prominently mentioned by our participants, and therefore was not included as a decision-making factor in our data. Thus, we do not see any convincing reason to separate Benefits from Purposes.

Benefits related to physical health and safety were mentioned very often by our participants (possibly due to the focus of the interviews, or their own concerns). Such benefits included safety and help in emergency situations:

> Why do I need to be tracked? Just in going around my daily life. Unless it can't work without doing that. Unless it's all or nothing. We can't send a message saying you need help unless we always know where you are. (P47)

medical diagnostics:

> For me it was very informative, the sleep rhythm because I do wake up and I was wondering how that influenced my sleep. And after wearing this I see not really, it didn't seem to influence it that much. (P26)

and incentive to exercise or take other steps to improve health:

> It motivates me to get out there five days a week. [...] There's not that competitive aspect to it and it is just helping to keep my weight down. (P8)

The intangible benefits include emotional support and feeling of connection:

> I live among old people and there are many of them that if you ask them what's bothering them, they couldn't tell you what is bothering them. So if there is a way for them to tell the smart speaker what's bothering them, then with the right understanding at the other end, be that a machine or a person, one could probably figure out what's wrong . (P121)

saving time and convenience:

> [Sending gifts] was much easier to do it with Amazon than any U.S. postage or anything. They wrapped it and shipped it and everything. (P32)

and recommendations of interesting or useful content:

> One of the reasons I don't do location is [...] I get the impression whenever they know where you are, they start telling you what restaurants are around, or what actions. If I need it, which I will in a foreign place, or city I'm unfamiliar with, fine. But I don't need it for [my neighborhood]. (P36)

6.4.1 Who benefits accrue to.

Purposes and Benefits > Who benefits accrue to

Participants were interested in **whether the recipient's purposes in collecting the data could potentially benefit them**, and/or ratified others they wished to benefit, as opposed to benefiting only the recipient. In the most straightforward cases, benefits accrue to the decision maker (and/or the data subject, if those are not the same person). For example, thanks to sharing some information, a decision maker can feel safer in emergency situations or through peer pressure motivate self to stay healthy and reach the goals:

> You have the goal and then you have to tell the group of people if you reach your goal if you did or not. Then there's the way you watch for each other. (P103)

Benefits may also accrue to the decision maker's close connections, such as family and friends. For instance, sharing personal information may educate or motivate other people, provide example or even be used as a role model:

> if someone asks, or you get into a conversation among men, say, about prostate cancer, and I've had an experience with that and I'm happy to discuss my experience but everybody's situation is unique to them and to what their doctors say. So it's not like I

> have answers but I am willing to narrate what I experienced, which by now, may be obsolete because medical science is moving so rapidly. (P6)

On the other hand, some participants were cautious about sharing information with other people to motivate them, because they did not want to annoy them:

> My niece [...] she resents anyone telling her anything about her diet. Of course, she only weighs three hundred pounds but that is fine, you know. She is just very hard-headed, so I don't tell her anything about my nutritional information or my opinions, (P104)

Some of our participants mentioned that even society as a whole can accrue benefits from using the information they share, for example, by advancing research, predicting trends, and affecting public policy:

> Don't think [nutritional data] needs to broadcast but... There is kind of a use for that, of knowing as, you know, as a society or group whether people are at least on the average getting the right amount to eat. (P28)

> You take the census every ten years here. [...] All of that information is available to the government. And the government has to have that in order to supply funds for schools and traffic and transportation and water, clean air. (P107)

The social component of helping others may sometimes even play a bigger role in the decision to share than personal benefits:

> I do all these types of [medical research] projects and stuff so that is good for me because if there is anything they find extra, they can also help me out, but I do it because it helps other people. (P33)

Decision makers typically negatively responded to the situations in which the primary goal benefits only the recipient (or the recipient's contacts), with minimal or no benefit to the decision maker (or even harm, as discussed in §6.5):

> People are greedy and have an agenda and you wouldn't want anybody who has that involved in the accumulation of this information. (P107)

In fact, even where there was an obvious benefit to the decision maker, they might still express some dubiousness if they felt the recipient was benefiting disproportionately:

> I don't particularly want my information, my preferences for marketing used. [...] the people that provide these devices want to benefit from the information. [...] 'Facebook is free!' so you give up all this information because it goes to advertisers. So lots of different things that used to be quote, technically free, they never really were, they were all monetized. (P71)

Note that in the remainder of the paper, by *benefits* we mean benefits that accrue to the decision maker or *ratified* others.

6.4.2 Perceived likelihood of benefits occurring.

Purposes and Benefits > Perceived likelihood of benefits occurring

Sub-factors contributing to this factor:

- *Data > Technology acceptance (§6.1.3)*
- *Data > Relevance to the recipient/goal (§6.2.1)*
- *Recipient > Trust in recipient (§6.3.1)*

A higher **perceived likelihood of any benefits occurring that would accrue to the decision maker or ratified others** positively affects the decision to share. For example, participant

P31 said she would be willing to share the information about the usage of her stove with a company that provides a service notifying people that they forgot to turn off the gas, *"because I had experience a couple times,"* so she expects that *"Maybe that's important to me."* Similarly, participant P102 said she would be comfortable to share information about her presence (i.e. in what part of the house she is)

> Because like kitchen and bathroom, those are the places that is more dangerous that my fall. (P102)

Unknown benefits tend to be judged as less likely or compelling than known benefits:

> I would have a little bit reservation because I'm more, as I said, proactive. I would like to know that the [medical] monitoring was being done for a specific problem rather than an unknown problem. (P21)

6.4.3 Extent of benefits.

Purposes and Benefits > Extent of benefits

Sub-factors contributing to this factor:

- Importance or added value for the party who accrues the benefit
- Urgency or time sensitivity of receiving the benefit

The **extent of benefits** describes the perception of how helpful overall the benefits could be, for example in terms of their *importance or added value* for the party who accrues the benefit, and/or the *urgency or time sensitivity* of receiving such benefit.

Importance or added value is often a driving factor for adopting the technology in general:

> If it is not useful to me and it is going to take up all this time, I don't think I want to waste my time. I will do the technologies that have an actual utilitarian function in my life, my life as an older person who has a little bit different needs than a younger person. (P47)

and for using it for information collection and sharing, specifically:

> [The wrist-wearable pedometer is] obviously collecting information that somebody else is going to know about you. That somebody else is going to want to know. None of these things do I want to know. [...] I can't understand it. [...] If somebody's going to give up their privacy for a device like that, there must be a reason for it. So, I really don't care how many steps I take in a day. (P77)

The ***urgency of receiving a benefit***, like assistance in an emergency situation, affects the assessment of benefit extent, and sometimes even serves as a prerequisite for data sharing:

> *[I: Except your doctors, who or what else would you expect to request access to this data?]* Nobody... unless I was incapacitated for some reason and my sister might need access to my doctors or to information; if I went into a coma. She might need to know who my doctors were. (P1)

> No, I wouldn't object to it [the device] having all this information. It's private information right? I mean they're not going to put it on the Internet or anything [chuckles]. It's personal, private information for an emergency, or my doctor, or that. Or whoever is controlling this. (P10)

⇆ Connections and Trade-Offs ⇆

Participants often referred to the trade-off between privacy and personal value, for example, for ride-sharing services or social media:

> When I go in the city, instead of getting on the bus, it is easier call Uber. [...] It is such a convenience. That is what this modern world is, you have to weigh giving up your identity at a certain point versus a convenience. [...] Are you lazy enough, you want the convenience and the quickness, or do you want to do the old fashioned way and have your privacy. What privacy is left, anyway. (46)
>
> Then when I hear the latest news stories about Facebook this or that– [...] well, I don't have to be scared because I'm not really, I'm sort of keeping myself away from that world. But then the reverse side of that is, am I harming myself by not taking advantage of all this stuff? Am I limiting my life? (P47)

As we noted in §6.1.3, assessment of *importance or added value* may also be related to *technology acceptance*, particularly *circumstances that increase the need for collection and sharing*. Many participants were not willing to share their data, not due to privacy concerns, but because they did not expect it to be useful yet. However, they might be open to the idea of using it in the future, or to use by other people in more precarious conditions:

> You know, I could see use for these things [technologies] if I were more frail or if I were alone but I don't, I don't think of myself as needing help in those areas. *[I: Do you mind if certain devices are able to do this, or...?]* Oh, no. No, it doesn't bother me. (P18)

6.5 Risks Dimension

Factors in the **Risks** dimension:

- Perceived likelihood of negative consequences
- Potential severity of consequences
- Who accrues the consequences

The Risks dimension describes the potential threats associated with data sharing. Typically, recognised risks negatively affect the decisions to share data. For example, when the decision maker anticipates that her data may be misused, she is less likely to share it. In contrast, sometimes the absence of such recognition may positively affect the decision to share, for example, if the decision maker does not imagine a scenario in which the shared data may be misused, she may be more willing to share it:

> I've never had a problem, so I can't say that I'm really concerned about it [personal information]. And I think that I'm in an older age group where I think they are not as interested in you because they probably don't see you as a major consumer. (P110)

Similarly to the Benefits dimension, we distinguish three main domains of information sharing risk consequences: material, physical health and safety, and intangible risks. Material risks presume material loss or damage, such as financial losses due to credit card or identity theft, property damage due a robbery facilitated by the misuse of shared data, exposure to liability, or loss of financial or other material benefits to which the data subject was otherwise entitled. Risks to physical health and safety include assignment of a wrong medical treatment because of falsified medical data, attack by a stalker, or even death due to a hacked smart medical implant, such as automated insulin pump. Intangible risk consequences are immaterial in nature and often carry emotional or social effects, such as online harassment, government oppression, on unsolicited targeted advertising, leading to emotional distress, waste of time, or reputation damage.

We discuss in more detail the examples of risks in various domains, privacy and security concerns, and mitigation strategies that arose in our interviews in [49]. In contrast, in this article, we focus on the factors that affect the perception of risks, and how those risks impact the decision to share data. The factors that affect the perception of risks include: *perceived likelihood of any potential negative consequences occurring*, *potential severity of such consequences*, *who the consequences of risks accrue to*, and *ability to protect against or mitigate potential risks.*

6.5.1 Perceived likelihood of negative consequences.

Risks > Perceived likelihood of negative consequences

Sub-factors contributing to this factor:

- Assessment of whether the recipient's primary or secondary purposes carry risks
  - Expected material value of the data to the recipient
  - *Recipient > Trust in recipients (§6.3.1)*
  - *System > Data retention (§6.6.2)*
  - *Environment > Laws and regulations about information sharing (§6.7.3)*
- Assessment of the potential for risks unrelated to the recipient's purposes
  - *System > Connection to the Internet (§6.6.3)*
  - *Environment > Stories (§6.7.4)*
- Potential inferences from the data
- Reusability of the data across contexts
- *Data > Amount or extent (§6.2.3)*
- *System > Ability to control data flows and protect against or mitigate risks (§6.6.6)*

A decision maker may consider the **likelihood of any potential negative consequences occurring** due to information sharing. As we noted in our initial descriptions of the dimensions, such potential negative consequences may be related or unrelated to the recipient's purpose for information collection and use.

For the former case, the decision maker makes an ***assessment of whether the recipient's primary or secondary purposes carry risks***for the person who may accrue the consequences. This assessment in part depends on the *expected material value of the data to the recipient*. For instance, the decision maker, who does not imagine what value the recipient may extract from the shared data, is more likely to expect low probability of the information misuse:

> Trying to imagine like a scenario where someone might misuse information about your nutrition and I just can't really think of one. [...] I think people have better things to do than wonder how many calories a person eats per day. (P47)

On the other hand, if the decision maker is aware of how the recipient may use the shared info to extract personal value to the detriment of the decision maker, then she that may increase her estimate of the likelihood of the recipient exploiting the opportunity to misuse the information:

> *[about tracking sleep patterns]* My whole concern with a person trying to break into my home and steal things, maybe there are people out there who want to wait till you are asleep and then they try to sneak into your home [...] and they steal your stuff or whatever . (P47)

The assessment of likelihood of risks also includes not only the recipient's intended use of the data but also an ***assessment of the potential for risks unrelated to the recipient's purposes***, i.e. risks that are unintentional on the part of recipient but which the decision maker is nonetheless exposed to. For example, deployment and regular update of security safeguards and enforcement of privacy-protecting law reduce the likelihood of information risk occurrence:

> I don't know how to protect against that, unless it's the people who make this technology, you know, they install some sort of security system or something so that it is, you know, it's only accessible to the folk that really need to know it. (P47)

The likelihood of the risk may be higher in certain environmental conditions, for example on a public computer:

> I would never do [online banking], obviously, in an open environment, you know. So only at home. Not in public. (P104)

While participants appreciated free access to the Internet, for example in a cafe or public library, they did not recognise the threats posed by unprotected internet connection (such as Wi-Fi spoofing):

> You can use Wi-Fi, right, and it's like if I went to Starbucks, it wouldn't cost me anything. That's what I would do. I'm not paying $100 a month. (P10)

Some decision makers may underestimate the likelihood because trying to predict the risks associated with data sharing, they do not consider the potential misuse of inferred information:

> I rely on the GPS completely. [...] I'm not too worried about that. I mean if it asks, give us your zip code so we get your location, I put that in. (P18)

> I'm not seeing a psychiatrist. I think if I were, I wouldn't want anybody to know what I would be telling a psychiatrist. But I'm not, so, you know ... Doesn't make any diff [sic.] [...] as far as the medical stuff, such I tell you, it's boring. Why anybody would even look at it and find anything interesting. There is nothing. [...] I'm an old lady, doing hardly anything. (P43)

However, other participants noted that the likelihood of risks (especially of more severe risks; see §6.5.2) may depend not only on the direct meaning of the data, but also on the ***inferences one can make from this data***. For example, when we asked our participants what information they would define as sensitive, participant P9 answered:

> I just thought about location. [...] I'm in the closet, a bisexual guy. I go to bathhouses in [cities]. I don't really want to let the world know, even my immediate family. (P9)

Later we asked him how someone can misuse the information that he has been to a bathhouse, and he answered:

> Well, it could be interpreted. Surmised. (P9)

Especially, aggregated information increases the potential for deriving meaningful inferences that can be misused:

> I do not use Facebook, I do not use any social media at all. [...] I realize that if you put all of that information together, and you are so inclined that you could do an awful lot of harm. [...] We are today in a position to put data together and know more about you than you know about yourself. (P121)

Some participants believe that their political beliefs can be inferred from their browsing history:

> I use the computer to go to websites that are off the wall. [...] Why are they not approved, because Google thinks that they are not mainstream. [...] They will not send you to certain areas that are Socialist, or politically sensitive. [...] I save the websites that I want to go back to again and again. I have a folder of Socialists' websites. I have a folder of news websites. On the news websites, I am a political progressive, a liberal, a lefty. I guess some of what is behind what you may sense about me is that I am a Vietnam vet. (P60)

> So they know everything you are doing, they know what you are looking at, [...] searching for and everything else. [...] somebody could actually gather all that data

> and use it and say well this person is a nasty democrat or left-wing or right-wing or whatever so that is the only thing concerning about the smart speaker especially. (P33)

Participant P104, for instance, stopped expressing her support of political candidates or news outlets on Facebook due to her concerns that her political beliefs can be inferred this way:

> I saw Elizabeth Warren or whatever [...] or Daily Kos– I would do a like, or submit, and now I've decided not to do that because you just don't know what's being captured. But I really want to support those people." (P104)

Another example of an increased risk is associated with the ***reusability*** of seemingly non-sensitive data, e.g. for authentication:

> I had identity theft last year, by the way. [...] [They] opened an account in a couple of department stores, hit my Macy's account [...] *[I: Do you know how that happened - what led to that?]* Nope. They had the right birthday– and which, don't ask me. (P36)

6.5.2 Potential severity of consequences.

Risks > Potential severity of consequences

The **potential severity of consequences of a risk** involves the extent of undesirable consequences it may entail, in terms of financial or time loss, material or health damage, emotional impact, etc., depending on the domain of the consequences. The severity varies from annoying:

> Oh yeah, you get a lot of weird calls when you are a senior in a rest home. (P108)

to significantly time-consuming and/or financially damaging:

> I don't want identity theft. I hear it's a total nightmare. Takes two years, you know, to get it straightened out. (P10)

and even to life-threatening:

> *[I: How do you think this recorded conversation or medical records or location or activity level or anything can be misused?]* Well, people can spy on it and then they want to come in and kill you. They want to know when there is no sound and you are asleep, then they come in. (P37)

6.5.3 Who accrues the consequences of risks.

Risks > Who accrues the consequences of risks

Similarly to the people who accrue the benefits, those **who accrue the consequences of risks** may include the decision maker, her close connections, society as a whole, and recipients. Most of the previous examples in this section depicted the negative consequences accrued to the decision maker as the most obvious impacted person. Participant P32 illustrates an example of negative consequences accrued to close connections (herself), whereas her stepdaughter is considered a decision maker sharing embarrassing information about the participant's stepgrandchildren on social media:

> My stepdaughter is lovely and I love her to death, but unfortunately her three children are at the lowest level that you can be in our society and it creates havoc of all kinds and it is very hard for me. [...] My step-daughter, she talks about it on social media all the time, but I would be horrified if everybody that is in my social strata knew what is going on. (P32)

An example of negative consequences accrued to society is the manipulation of presidential election results due to use of information shared by people on social network:

> *[I: Do you have any concerns about using Facebook?]* Yes, Given all of the ads that I saw during the [presidential] campaign, the last campaign. That was such a distortion of truth and people believed it. My cousins believed it. (P108)
>
> It could be some political group just like we have right now currently in politics [...] and they are trying to screw the voters over in this country [...] If you got enough money, you can hire a group of people to hack into anything now. (P33)

Recipients may also accrue the negative consequences of risks. For example, the device manufacturer or app developer have to pay a fine for violation of the privacy regulation, banks have to incur costs of credit card re-issuing following a data breach in which the credit card numbers are compromised, and entities who violate the privacy law have to face the legal retribution:

> With Facebook and different ones that have had all the information stolen from them– [...] there is a few lawsuits or politicians taking action against these people. (P33)

However, in our interviews, potential negative consequences accrued by the recipients are rarely given much weight in the information sharing decision making process, and are rather judged as an appropriate consequence if they fail to protect the data.

6.6 System Dimension

Factors in the **System** dimension:

- Decision maker's experience of sharing
- Data retention
- Connection to the Internet
- Human involvement
- Transparency about data flows
- Ability to control data flows and mitigate and protect against risks

The systems that decision makers may consider sharing data with or through may include (but are not limited to) hardware devices, software, mobile application, etc. The System dimension describes how a given system collects, transfers, stores, and uses (including processing and sharing) data, in terms of both policies and actual methods.

6.6.1 Decision maker's experience of sharing.

System > Decision maker's experience of sharing

Sub-factors contributing to this factor:

- Intrusiveness of the data collection practices
- Usability of the system
- *Decision Maker > Technology acceptance > Technology self-efficacy (§6.1.3)*

With respect to **decision maker's experience of sharing their data**, the decision makers evaluate the *intrusiveness* (especially interruption) of the data collection practices and *usability* of the system.

Intrusiveness is typically related to an active involvement of the data subject in data collection and is negatively judged by them

> I think the watch is great [as a heart rate monitor]. Because it doesn't affect what you do, it's like wearing a bracelet. (P107)

Note that by intrusiveness here we mean an interruption caused by the data collection practices rather than intrusiveness in the privacy sense.

If ***usability*** of the system is low, i.e. the effort required to use the system's data sharing functions is too high, the decision maker may choose a different channel or become reluctant to share information altogether:

> It has to have something that tells you how to use it. Which I understand the smart phones don't always tell you everything that the phone can do. You have to figure it out yourself. I have trouble with that only because it's so complex. (P5)

On the other hand, as discussed in §6.1.3, the convenience of using electronic channels encourages decision makers to share their information.

6.6.2 Data retention.

System > Data retention

The duration of data retention can be broadly categorized into limited (including until the purpose of data collection is met) and unlimited (including unspecified time period). Participants who mentioned data retention as a decision making factor typically preferred limited data storage over unlimited:

> I don't want them to keep anything there. Once I'm done is gone for my own benefit. I don't have to keep any record over there. (P103)
>
> I hadn't even thought about [hearing aid apps] collecting [data], or where all that stuff goes. I think it's only me hearing it. Phew. Is a record of that around forever? (P123)
>
> I didn't know that that was possible to retain information. [...] I thought it was just, you know, you told them [smart speakers] what to do. They did it and then, they were on the next thing [...] like recording over the tape [...] If you recorded over that tape, you wiped out pretty much what had been said or done. (P35)

6.6.3 Connection to the Internet.

System > Connection to the Internet

Sub-factors contributing to this factor:

- Transmission channel
- Hosting

Sharing data in person or over non–Internet enabled ***transmission channels*** is perceived as more secure:

> I got a new credit card and they wanted my social security number and I didn't want to give them my social security number. I had to call—I gave it to them over the phone. (P24)
>
> I don't believe in online banking, particularly. [...] Well, I do have one bank account that's online, but I do not have any of my stuff sent on the internet. I get printed copies. [...] Statements, credit cards bills [...] It's easier for me to look at them, compare, keep records—you know, to destroy. [...] I just don't want records out there. (P36)

On the other hand, some respondents find sending the information of the Internet more convenient (see *decision maker's experience of sharing*, §6.6.1). The convenience of online channels may outweigh the concerns:

> It is just like with my neighbor and my banking online [...] her writing checks and going to her private banker to check up on something rather than to go online. And the thing is that, you know, you move on with the times, so you may not like some of the things, but you can do only do so much and then you just go one with it. (P33)

One participant acknowledged however, that in the era of ubiquitous computing, it is hardly possible to avoid the digital connection between the online and offline worlds, because even if the decision maker does not directly interact with the technology, her personal information may still be collected and shared by others:

> All my charge cards, all my whatever, everybody knows exactly what I'm doing, even though I never put it on a computer. It's on a computer from someplace else. [...] Every phone call you make is recorded somewhere. (P4)

Hosting is a question of whether the data is stored locally (on the device or separate storage medium), or stored virtually (on a cloud service, the manufacturer's or third party server, etc.). Virtual transmission and storage raise more concerns among the decision makers than the local storage:

> The television, the smartphone, the speaker, smart speaker, the computer, they are all, most of them are hooked up to the internet[...] All that data goes back and forth to the internet, so it is all out there someplace in some server or something. (P33)

Those of our participants, who were aware of the difference between various hosting methods, typically expressed least trust toward the cloud storage:

> I would like to know where the financial information is, which computer has is. I don't want it on the Microsoft cloud, I don't want it on the Apple Cloud. I want it on a hard drive that I know is on that computer and the portable hard drive that is hooked up. I don't use a wireless backup, a cloud back up. So I guess I am really concerned about anything that has financial information on it. (P123)

6.6.4 Human involvement.

System > Human involvement

The **extent of human involvement** in data collection or processing and analysis varies between fully algorithmic and fully human processing. Human involvement is usually associated with higher degree of privacy concerns and human errors (cf. [**?**]):

> Like somebody works at the DMV and they looked up, address of ex-girlfriend or something, and then they've got out and hurt that person. [...] People that shouldn't have access to your records who are in an official capacity could use information about you that they happen to see. (P71)

> The person that is– actually that has the keys, knows the password to get into patients' database [...] maybe there could be a lot of things that would motivate them. [...] Maybe they've been messed over by their supervisor at Kaiser [the insurance provider they work for] and the way they are going to pay Kaiser back is compromising the patient information. Or maybe there is a particular patient that they want to get at. Maybe they want to get their ex-boyfriend's data and mess with it. (P8)

However, decision makers might have other reasons for preferring humans to be in the loop:

> *[about care robots]* I prefer communicating with people and being able to ask for what I need. (P28)

6.6.5 *Transparency about data flows.*

System > Transparency about data flows

Participants often mentioned the importance of **transparency about data flows**:

> I guess there would have to be an even playing field, a balance between those who are providing the device and those who are using the device, again a certain level of transparency that is not always there with businesses. Business looks upon something like this as proprietary and they don't want to share it. (P60)
>
> The same with medical records, I am pretty open with everybody about what is going on with me, but I don't want them to have access to that without me knowing. (P32)

On the other hand, some assumed (not necessarily correctly) that the devices' interfaces are accurate representations of what is being collected:

> I don't see my phone capturing my data, unless—what I enter. (P104)

In §7, we make some specific suggestions for effective disclosure, notices, and signalling.

⇆ Connections and Trade-Offs ⇆

In some cases, participants clearly indicated what elements of the system or aspects of the sharing scenario they would be concerned to have transparency about, such as recipients or purposes:

> I find myself starting to fill things in and then I get partway through. I get on the computer and I stop and I say, 'Eh, I don't want to give all this information. I don't really know where it's going.' And I stop and get out of the thing. (P18)
>
> I'd have to ask some questions first to see if the device itself was being used other than it was intended. Do I understand what the device is to be used for? (P60)

However, such clear, direct statements indicating that a decision hinges on the transparency of a specific element are relatively rare (in comparison with comments about a decision hinging on the factor itself or on transparency generally). We therefore do not include specifics about what participants mentioned wanting transparency about as factors or sub-factors in this section, because we do not have enough data to confidently pick out which are the elements of particular concern. Rather, we view *transparency* as broadly acting in combination with other factors elsewhere in the model to constitute complex decision-making factors. (Same principle applies to the *ability to control data flows and mitigate/protect against risks*, §6.6.6.)

6.6.6 *Ability to control data flows and mitigate/protect against risks.*

System > Ability to control data flows and mitigate/protect against risks

Sub-factors contributing to this factor:

- Existence and availability of relevant means of control/protection/mitigation
- Cost of control/protection/mitigation
  - Monetary cost
  - Required time and effort
    - *Decision maker > Technology acceptance > Technology self-efficacy (§6.1.3)*
- Likely effectiveness of the means of control/protection/mitigation

Participants mentioned concerns about being able to protect themselves against the risks of data sharing or mitigate negative consequences, as a factor in their decisions about whether to share (i.e. whether to accept the risks). Risk protection is closely entangled with **the ability to control data flows**, in that data being collected or shared in ways the decision maker does not want constitutes a risk in itself. Therefore, protecting against or mitigating risks often involves controlling data flows, either for its own sake (i.e. protecting against the risk of unwanted data flows within or from the system) or to prevent secondary risks.

To assess ***the existence and availability of relevant means of control/protection/mitigation***, the decision maker may consider whether (to their knowledge) the system provider has taken steps to ensure control, including security and privacy of the data practices:

> I trust Apple more than most anyone, their security seems, you know texting your codes or sending a code to one of your listed devices, well if you sign into iCloud if you have that two-layer security turned on, whatever that is called, that's pretty secure stuff. And they are pretty resisting. You can't just copy anything you want onto a phone. On a Windows computer you can copy anything you want to. So they [Apple] have pretty good security. (P123)

> Can I specify who I share with? Like Facebook where you can say, 'these are my friends.' (P24)

The decision maker may also consider means of control, protection, and mitigation that can be added on from entities outside the system, such as physical security tokens, anti-virus software, or anti-tracking extensions:

> I used to have antivirus but now it's built into Microsoft, so I use Microsoft. (P108)

> I would say get a call blocker[...] Once I attached it, I saw that there were some numbers calling and immediately the call blocker showed up that it already deleted two of them. (P110)

or that are completely external to it, such as identity theft protection services; the latter we cover in §6.7.5.[5]

The decision maker may also assess the ***cost of controls, protections, or mitigations***, in terms of *monetary cost*:

> I gave money to a firm that said that they would provide some protection for my [...] brokerage account. I don't know whether really that they would be that effective. [...] Probably a waste. (P51)

(Although our participants did not mention it extensively, prior research has shown that users expect more privacy protection, transparency, and control from the paid versions of the online services (e.g. smartphone apps) than from their free counterparts [13].) They might also evaluate cost in terms of *required time and effort*, which reflect the convenience and usability of settings interface:

> It's hard enough for me to come up with a password that I can remember and not write down– they tell you not to write it down so I don't do that. (P110)

Time and effort required to protect against risks is often weighed against benefits:

[5] We include such measures here, under the System dimension, because they eventually have an impact on the decision maker's ability to control the data flow, mitigate and protect against the risks, while using the system. In addition, whether a decision maker views a protection as being internal or external to the system depends on what they conceptualize as being part of the system in the first place.

> Sometimes when I go on the computer to check on things, it will say do you want to keep this password, I always say no, because I will change. And it is a hassle, but it is just a second, it is just a precaution, you know. (P46)

In some cases, the difficulty of controlling specifics leads to a categorical decision not to share:

> *[I: How would you expect this new system, or will want this system, to address privacy and security concerns?]* By making it very, very limited to my doctor, my daughter, and the emergency people. That's it. And if it can't be controlled that way, then I don't want it. (P10)

Participants also had questions about ***how likely protections are to be effective***:

> I have to assume they have security devices build into the programs, and they are not always effective against hackers. (P77)

> You purchase this anti-virus stuff that you put on there but it seems like they are not able to do the work. If someone is bent on wanting to get into your data or whatever device. That is pretty freaky. (P53)

> I don't think you have much choice. You can block an ad on Facebook but then you'll just get a different one. (P108)

In §7, we make some specific suggestions about system elements and functions that decision makers could be given more control over.

⇆ Connections and Trade-Offs ⇆

For a decision maker's choices to depend on the existence and availability of means of controling data flows and protecting against or mitigating risk, the decision maker must be aware of them. The model does not attempt to account directly for a decision maker's lack of knowledge about any specific control or protection, as it only describes factors the decision maker could be aware of. However, some participants expressed a higher-level awareness of how their general lack of knowledge about protections could affect their decisions, in terms of *Technology self-efficacy (§6.1.3)*:

> I'm not sophisticated when it comes to all these electronic gadgets and so I don't know what the possibilities are for control that is unavailable to hackers and thieves. (P20)

6.7 Environment Dimension

Factors in the **Environment** dimension:

- Norms about appropriate or usual *behavior*
- Norms about appropriate or usual *information sharing*
- Laws and regulations about information sharing
- Stories about information sharing
- Alternative options for achieving the decision-maker's goal

The Environment dimension includes factors describing the external context of the information-sharing decision-making, not directly related to the System and its users, such as *norms about appropriate or usual behavior*, *norms about appropriate or usual information sharing*, *laws and regulations about information sharing*, *stories about information sharing* that the decision-maker may have heard from the media or close connections, and *alternative options for achieving the decision-maker's goal*, outside of the System.The Environment dimension is distinct from the System dimension in that designers and developers have greater control over factors in the system dimension, while environmental factors should be taken into consideration but cannot be directly manipulated by the designers and developers.

6.7.1 *Norms about appropriate or usual behavior.*

Environment > Norms about appropriate or usual behavior

Sub-factors contributing to this factor:

- Behavioral norms within a specific small group/community
- Broader social norms of behavior
- Laws about behavior

Norms about appropriate behavior or usual behavior in a given context may influence a decision maker's judgment about whether they are comfortable sharing data because of the content it captures. Our participants often mentioned that they are open to collection or sharing of information about activities that comply with sociocultural **norms about behavior**—whether ***small-group or community norms*** or ***broader social norms***—and reluctant to share information about behaviors that violate such norms:

> *[I: What kinds of information [would you] be sensitive about if these devices collect about you?]* I don't think of myself as a mainstream person. In the bell-shaped curve I am not in the middle. [...] Because I'm marginal, I'm suspect. [...] I'm very interested in socialism. (P60)

> Since I'm not involved in anything illegal or improper, that wouldn't bother me [to have my conversations recorded], but I could see why it would bother some people. [...] In something illegal or improper such as having an affair. (P110)

In particular, with reference to ***Laws about behavior***, participants often used proof of illegal behavior as a paradigm example of sensitive data that someone might not want to share:

> You're not trading any gold bar or trading marijuana so I guess it is not sensitive. I mean unless you are and conducting spying activity, you know. Or if you want to do some underhanded thing, you know. You have some secret mission—I don't have any of those, so... (P37)

⇆ Connections and Trade-Offs ⇆

In addition to concerns about sharing information explicitly about activities or characteristics that do not comply with *norms about behavior*, a few participants were concerned about how *inferences from their data* (§6.5.1) could indirectly put them at risk for judgments about not complying with social norms:

> Well the computer could know, you're being addicted, you have a compulsive thing. You've been on this too long. You've been researching this current thing to death. (P9)

6.7.2 *Norms about appropriate or usual information sharing.*

Environment > Norms about appropriate or usual information sharing

Sub-factors contributing to this factor:

- Information-sharing norms within a specific small group/community
- Broader social norms about information sharing

Sociocultural **norms about appropriate information sharing in a given context** may relate to whether it is appropriate to collect/share information about a particular topic, with whom it is appropriate to share it, or other contextual factors—for example, sharing photos posted on a social media with an employer vs. with a friend. Such norms are often specific to the expectations in a particular context. For instance, our participants mentioned that it can be appropriate to collect a specific piece or type of data in a public place or where there is a large group of people, but not in a more private setting:

> I guess if you go to a public place then it is not sensitive, you know. (P37)
>
> So maybe you would be fine to [have the smart speaker] record [...] [of] everything happening at a party because [...] it isn't private. But then the party is over and you know, you are cleaning up and all of a sudden, the conversation after is a whole different conversation. [...] if that's recorded maybe you wouldn't want that. (P34)

Some norms can be perceived as ***specific to a small group, community, culture, or generation***:

> I was in– waiting for a bus and a young lady was waiting for a bus. [...] She's sitting there in the bus stop, giving a blow-by-blow description of her sexual life to whoever was on the other end. [...] I don't need to know that they just had an abortion, or that [...] they have a husband that's cheating on them or something. Not my business. [...] I may sound– I'm not going to say "old-fashioned," a little jaded, but I'm finding the younger generation is like, everything is in your face. (P36)
>
> I also wonder if there's a generational thing. Because I just hear people being interviewed on TV where 'Oh, I'm not so concerned about Facebook's breach' [...] Where people my age that have grew up under a different system, have more concerns about it. And other people who are more accustomed to [...] or work in tech, probably have a different feeling about it. (P71)

Alternatively, norms may be ***defined by the broader society*** and may cross cultural borders. For example, participant P24 shared her opinion about similarities in norms of information disclosure between various countries in Europe, but contrasting them with the US:

> I lived in Sweden and in Germany when I was young. In both countries I had to register with the police [...] I had to have a living permit, obviously. But the police had to know where I lived. When I moved I had to sign in. And that was really hard in the beginning. Because in America, in the States, people shouldn't be knowing that. [...] at that time in America, people, other Americans got really enraged. (P24)

⇆ Connections and Trade-Offs ⇆

Norms about information sharing are often closely linked to *norms about behavior* (§6.7.1), in that it is often viewed as inappropriate to observe or share information about inappropriate behaviors. In fact, they may be difficult to distinguish; for example, it is unlikely that P32 finds using the bathroom inappropriate, but it is not clear whether she views nude housecleaning as inappropriate to do or inappropriate to observe:

> I mean, I don't do anything that I care. I mean, I wouldn't let it view me in the bathroom maybe, but I don't clean house nude or anything. (P32)

6.7.3 Laws and regulations about information sharing.

Environment > Laws and regulations about information sharing

Participants also referred to **laws about information sharing**, not only in terms of concern that their own sharing of information might be illegal, but in terms of potentially being more comfortable if they thought recipients would be bound by those laws:

> Medical records, well, there's HIPAA restrictions. (P104)

In contrast to sociocultural norms, legal norms impose tangible financial and criminal liability for violations (see §6.5.3). Where respondents perceive a lack of regulation, they might express an aspiration or need for it:

> [Politicians] would have to set laws about access and priorities and privacy and all that sort of thing. So, and then to call committee meetings and get the CEO and whoever is it and grill them. (P33)

6.7.4 Stories.

Environment > Stories

Sub-factors contributing to this factor:

- Current media stories
- Past experiences of decision maker's close connections

What the decision-maker has heard about privacy and information sharing, for example from ***current media stories*** (e.g. TV, newspapers, radio) or about ***the past experiences of their close connections***, also affects the security and privacy attitudes and decision to engage in information collection or sharing:

> When I heard about Facebook, I was worried about it. (P20)

While many participants mentioned hearing about privacy and security violations, they don't necessarily know or remember details about how the violation occurred:

> I have a friend of mine, I know of somebody in the building that had trouble with that, and somebody else. [...] He's trying to put his life back together when somebody stole his identity. *[I: What happened?]* I don't know, I haven't seen. I just, he said it's a mess. (P77)
>
> The stuff I've been reading about [Amazon Alexa smart speakers] in the newspaper, the last couple of days, about them overhearing conversations and acting on them. *[I: Acting in what way?]* I don't know, detrimental to you. I mean, there was one in the paper the other day that sounded terrible. I can't remember it. (P77)

Some participants were skeptical about whether the media is a helpful source of information on this topic:

> I think they can capture more information– I don't know enough, but I just saw something on TV, or whatever, and they said it's– of course, you know the news is all about trying to scare you so you don't go anywhere, or do anything, or think. [laughs] (P104)

particularly because of the difficulty to distinguish fake news from legitimate news:

> *[I: Where did you hear about [...] being vulnerable using Wi-Fi in the coffee shops? [...]]* Oh, um, on the news. I think on the news and—is that fake news? See, this is all new to me, too. This new fake news because you shouldn't believe that—it's fake news. (P34)

6.7.5 Alternatives.

Environment > Alternatives

Sub-factors contributing to this factor:

- Existence / availability of alternatives

- Cost of alternatives
  - Monetary cost
  - Required time and effort
    - *Decision maker > Technology acceptance > Technology self-efficacy (§6.1.3)*
- Likely effectiveness of the alternatives
- Preference for in-person communication

In addition to evaluating whether a particular system, device, or app really *requires the requested data to perform its functionalities* (or whether it could function without that data; see §6.2.2), a decision maker may also consider **alternative ways to achieve their goal**, outside the system in question:

> I do not use Twitter or email much at all. I prefer Kaiser, for instance, to send me a postcard and/or a phone call [for an appointment reminder]. (P69)
>
> There are devices that use GPS and show where you are. That's also something I can do in my mind, I can look and see where, or look on the map. *[I: So you don't use GPS for directions or anything?]* No. *[I: And it's because you already know how to get somewhere? Or you don't feel comfortable sharing your location?]* No problem sharing the information, no. (P28)

The viability of alternative means for achieving the decision-maker's goal depends not only on its ***existence and availability***, but also whether the decision-maker views it as desirable to use. Participants mentioned that they choose alternative methods for achieving the goal depending on how they compare in terms of *monetary cost* or cost-efficiency:

> I think [smartphones] are expensive, probably. [...] I'm afraid of losing it. They are a big theft item. Nobody wants my flip phone. It's very safe. (P15)

convenience and usability, expressed in terms of *required time and effort*:

> I do all my banking online. I enjoy that, no more envelopes and postage stamps and having to go to the post office. I like that lot. And then I can always get reports immediately on the status of my income and the status of my spending. (P22)
>
> I tried [the tax preparation software] and I think I could not, found it difficult to do changes or something. I just gave up. Thank God they still accept the paper form to do taxes. (P7)

as well as ***effectiveness*** in reaching the decision maker's goals or achieving the maximal benefit:

> I don't do any monetary transactions online at all. [...] I just don't think it is particularly safe. [...] Another reason is I'm quite satisfied with Trader Joe's [grocery stores]. [...] I just like to go and see what I am getting and smell it, or even get a sample. (P25)

Decision-makers may also choose alternative methods based on ***whether they generally prefer to communicate particular information in person***, or via a maximally personal channel:

> When you are having a private discussion with someone, you ought to be able to feel that it's as private as those that are involved in it are willing to be, you know. You can't obviously be sure that they won't go blabbing it all to the next person they talk to, but I wouldn't want technology doing that for me. (P15)
>
> I think that [social media] is time consuming and if I want to know what my friends are doing I want to talk to them in person. [...] I don't want to put information out for a network of people. I don't want everybody to know the same information. (P32)

⇆ **Connections and Trade-Offs** ⇆

Alternatives to sharing, or alternative modes of sharing, sometimes came up with reference to *circumstances that increase the need for sharing* (§6.1.3). For example, a decision maker might be facing a choice about whether to share data with an online device or system or continue to use an offline system due to some special circumstance or need:

> If you are concerned about your mother and you can't be there 24/7 and you want to make sure she is okay, [a care robot] sounds like a good idea. *[I: Would you be comfortable using a care robot?]* Not right now. I don't need one. [...] I belong to care insurance, so I would probably have a person physically come into the house. So I don't know. I'm not at that stage. (P108)

In considering alternative means to achieve the same goals, participants might compare the *likelihood* and *extent of benefit(s)* (§6.4.2, §6.4.3) they might achieve under the different scenarios (see *effectiveness* above), as well as the perceived level of *Risk* (§6.5) associated with each:

> When nobody was looking, they come around and jimmy the [mail] box open and take these checks. [...] And I said it is the same thing as being on the Internet and somebody gets into your bank account and tries to take money out of it, it is the same. (P33)

> *[about a medication dispenser]* Who would ever trust anybody but me to my own medications? I'm really very careful with them. I want to control them. I still want to control them. Too many things can go wrong. I take too much stuff. (P77)

7 DISCUSSION AND FUTURE WORK

In this section we discuss the theoretical contributions and practical implications of our model, as well as future work on its extension and validation.

7.1 Theoretical Contribution and Research Extensions

We first compare our model to existing theoretical frameworks on information sharing, and then describe the applications of our model in research.

7.1.1 Comparisons with existing theoretical frameworks. In this section we outline the similarities and differences between the existing theoretical frameworks for information sharing and our model. For the most part, our model is compatible with each of the reviewed theories, though they may have a narrower focus or look at information sharing from a different angle. Our goal in this paper is not to argue against previous theories, but to provide a comprehensive model that is broader in scope, applicable to a wide variety of situations, and offering a greater level of details regarding the particular contextual factors that may affect information sharing decision-making.

In the focus on contextual factors, our model shares the most similarities with the Theory of Privacy as Contextual Integrity (CI) [87, 89]. In some cases, the CI parameters correspond to high-level dimensions of our model; for example, 'recipient' is an element in both. In other cases, factors in our model overlap with the CI framework, but relate the analytical constructs in a different way. For example, contextual norms for information sharing and norm-based privacy expectations are the main object of inquiry in CI. In our model, *privacy norms* and *privacy expectations* are two among many pertinent factors of a sharing situation that may be weighed in decision making.

On the other hand, our model provides a more detailed structure for describing a broad range of elements that are bundled under the heading 'transmission principles' in CI. Specifically, our model elaborates a structure of data-sharing factors and sub-factors under the dimensions of *purposes and benefits* of sharing, potential *risks*, and elements of the *system* data is shared over. This breakdown allows us to more closely examine the relationships among those factors and sub-factors. While there were some attempts to empirically study the impact of certain transmission principles on information-sharing attitudes and intentions [72, 73, 104], to the best of our knowledge, no one has offered a systematic theoretical framework for transmission principles. In addition, the granular description of factors can help to systematically evaluate existing systems and information-sharing policies to identify potential points of intervention. It can also provide an accessible starting point for designing systems that (for example) better respect contextual norms (see §7.2.5).

As with CI, our model is compatible with Communication Privacy Management Theory [75, 92, 93] and Altman's Boundary Regulation Theory [7, 8], but has a different scope. Both of these approaches to boundary regulation analysis of privacy focuses in-depth on the balance between goals (avoiding intrusion when sharing the information publicly vs. avoiding loneliness when keeping the information private) and how that balance changes from situation to situation. Our model applies to a wider variety of goals that decision maker and recipients are trying to achieve, from personal goals of monitoring health, or protecting the loved ones from excessive worrying, to the broader goals of advancing research or improving the companies' services.

Our findings include the factors pertinent to protection self-efficacy, and perceptions and severity of privacy threats outlined in Protection Motivation Theory [98] and Technology Threat Avoidance Theory [67]. However, we also include contextually sensitive factors in other dimensions, not related to risk (such as benefits of information sharing, trust in recipients' intentions, etc.).

Benefits and costs, central to the Privacy Calculus (PC) approach [38, 39], correspond to two of the seven dimensions in our model (*benefits* and *risks*), but again, we consider a wider range of contextually relevant factors and trade-offs. For instance, in contrast to PC, our model does not presume that the decision makers are fully rational agents, and allows information asymmetry, lack of transparency, meaningful choice or technological self-efficacy to hinder the informed decision making about information sharing.

In sum, some of our factors and dimensions align with elements that are explained in depth by other models and frameworks, and is broader and more comprehensive. This is partially due to the fact that we addressed a different research question: we seek to empirically account for the factors that may be involved in a decision about information sharing, rather than to analyse exclusively the norms and expectations, or costs and benefits of information sharing and disclosure. On the other hand, our model did not originate as an extension of the existing theories and was developed independently using a bottom-up analytical approach. Therefore, the partial overlap of factors between our model and other frameworks (particularly CI) shows the convergence of independent efforts to systematise an understanding of privacy-relevant contextual factors, and supports the potential validity of the proposed model.

7.1.2 Applications of the model in research. Our model attempts to systematize evidence about the impact of various factors on information-sharing decision making. Having a broad, comprehensive model of factors provides a foundation for comparing and consolidating empirical studies, and for connecting existing theoretical frameworks that focus on different subsets of the factors.

Our proposed framework can be used by information systems, privacy and security, and HCI researchers to:

- Further advance understanding of the complexity of information-sharing decision making, including the relations between contextual factors, and their valence and relative importance.
- Systematically review and compare existing literature and empirical evidence on the topic, controlling for the contextual factors.
- Design empirical studies (such as survey instruments, interview protocols, vignette scenarios, experimental design, etc.) that will analyse users' attitudes, preferences, decision making, and behaviors, while systematically accounting for the contextual factors and validating their effects (see §7.2.5).

- Design and validate new prototypes for transparency and control mechanisms for data sharing practices, and evaluate existing ones (such as disclosure, notice, and consent dialogues, and control settings user interfaces) along the dimensions and contextual factors outlined in the model. Such research can inform future product design (see §7.2.1).
- Design and test new interventions, and evaluate existing ones, for educating users about data collection and sharing practices, and for informing their decisions in that space. Such research can inform future interventions in consumer education. (For more suggestions for awareness and education programs and outreach targeted to older adults, see [49]).
- Design and test interventions, and evaluate existing ones, for educating system designers and developers about improving solutions for transparency and control. Such research can provide or improve practical tools for designing usable systems that empower users' informed choice, meet their expectations, address concerns, and allow them to tune systems to their preferences (see §7.2.4).
- Evaluate existing policies and regulations about data transparency, protection, and control, and inform improvements in regulation enforcement and control mechanisms (see §7.2.2).

7.1.3 Future work: Validating, extending, and integrating the model. In future work, we plan to validate and refine the model in a quantitative survey study, possibly incorporating vignettes (cf. [74, 85]). Such a study will quantify the predictive power and relative impact of the model's factors and sub-factors, along with the interactions between them. We also plan to expand the research and validate the model with other audiences (e.g. younger users, medical professionals and caregivers, seniors' family members), and with respect to various systems (including emerging wearable, healthcare, and smart home technologies along with more traditional ICT).

Additionally, based on the systematized combined theoretical and practical contributions of our model, theoretical models and frameworks relating to the general population (including the ones discussed in §2.2, such as Contextual Integrity, Boundary Regulation Theory, and Privacy Calculus), and other empirical work with older adults (such as that discussed in §2.1.2), we plan to help account for how people weigh the different contextual factors in practice. In addition, we plan to relate our model to other theories of privacy and security behaviors, such as the Elaboration Likelihood Model [94], the Theory of Reasoned Action [47], the Theory of Planned Behavior [4], and Behavioral Decision Theory [101].

Finally, future research may focus on building a database of resources that would aggregate the knowledge, including theoretical and empirical evidence, and best practices on each of the parameters in our model, to facilitate the search of relevant information for researchers, practitioners, system designers, and policy-makers. (While we provide some recommendations in the subsequent sections, it is outside of the scope of this paper to build a comprehensive library of resources.)

7.2 Practical Implications and Proposed Interventions

Having set out to describe how older adults make decisions about online information sharing, we find ourselves with an extensive, complex model with a broad ecosystem of interrelated factors. As expected, we did not observe unequivocal opinions; if any, the most common pattern of responses to the questions about information sharing preferences and decisions was "It depends." Therefore, we believe that scrutinising and quantifying the model (as described above) will provide useful mapping and insights into how the decisions depend on factors, how those factors are weighted, and whether they have strong valences. Such mapping and insights in turn will help to inform the design of technology, beginning with those aimed at older adults, and what limits there should be on data flows through those technical systems.

In this subsection, we sketch out some practical implications of this complexity for stakeholders with various goals: designers, developers, and providers of technology; policymakers; and educators. We then propose future work to support those stakeholders, and other researchers in addressing these questions.

7.2.1 Implications for product design. Technology providers have incentive to engage older adults in using their products—and to keep those users, rather than having them give up on using the product because it is too intrusive, unusable, or creepy, as shown, for example, in Frik et al. [49]. But a complex, context-dependent model of widely varying preferences and conditions on information-sharing does not present a simple answer as to how to accomplish that aim. There is no one best way to design a product that will make all older adults feel comfortable sharing data with it. Of course, developers need to ensure an adequate level of technical protection against severe privacy and security risks, as it is one of the most common expectations in our study. Although regulations attempt at defining the common legal boundaries, they are still too far from providing the adequate guidance for product design that would meet context-specific preferences. Therefore, while it is important to comply with the data regulations, we suggest not to limit the definition of privacy to the compliance with only technical and legal requirements.

A reasonable first step in approaching user-centric design solutions is to build trust with the user by being transparent, clear, and honest about the goals of data collection and use and recipients with whom the data is shared, as those are two main factors mentioned by merely all the respondents. Moreover, trust is one of the main conditions for older adults' adoption of ubiquitous computing technologies [29, 34, 80]. The goal of providing transparency is not only to build trust, but also to help users make informed choices and take informed actions to achieve their goals in a way that feels comfortable to them. In particular, transparency about data flows can support older adults' ability to understand the data sharing scenario and potential consequences, and from there, potentially their acceptance and use of a given technology.

It is important to adopt a user-centric approach in designing collaborative systems—such as fall detecting, home monitoring, and other systems in the health care context—because, as discussed in §1 and prior literature [e.g., 49, 90], the trade-offs between safety enabled by surveillance and associated violations of privacy often result in the conflicts of interests and conflicts of preferences among older patients and their family caregivers.

However, transparency without choice is not enough to address the concerns, therefore designers are encouraged to incorporate in the systems the mechanisms for user control over data flows that are unambiguous and easy to find and use.

The designers may rely on a body of knowledge and guidelines [e.g., 35] to address the identified issues and needs; we provide some recommendations in the remainder of this section.

Transparency and disclosure. Prior research has extensively studied the performance of different notification mechanisms and channels, and associated usability issues, including attention, habituation, risk communication, and comprehension issues [e.g., 9, 109].

For disclosure and notices to be effective, they should be provided at a time and in a manner that makes their relevance clear. While decision makers do not necessarily want to be interrupted with a notification each time their data is collected or shared, previous research has shown that current channels are inadequate [45, 112].

In addition, descriptions and signalling mechanisms should be simple and comprehensible to a layperson [77]. Notices should be specific about what data is being collected, used, and shared, who will receive the data, what are the recipient's purposes in collecting the data, what mechanisms or methods will be used, whether there are any known risks and, if so, what protective measures are in place [53, 61, 121]. Participants often mentioned concerns about not knowing these details about what was happening to their data.

Moreover, transparency without control mechanisms often lead to take-it-or-leave offers, which is especially problematic in monopolistic markets where users do not have enough alternative services, or are subject to lock-in effects. Therefore, adequate mechanisms for exerting user control are needed, for instance through more granular consent or improved user settings.

Control over data flows. Our participants expressed an extensive desire for control over personal information (see §6.1.4). However, the ability to control data flows is currently heavily dependent on the architecture of the technological system, introducing an asymmetry of power over this factor in favor of technology providers. Such asymmetry of power, as well as lack of transparency, often leads to privacy fatalism and resignation on the one hand, and to technology avoidance and reactance, on the other hand [49]:

> When you get Uber, if you don't log out and sign off each time, they know where you are all the time. I am paranoid about that. I don't like that at all. *[I: So, what are doing about that, do you still use Uber?]* No, I don't. No, I don't. I am trying not to use it. (P46)

Because developers have control over the system they design (and not over users), their primary attention should be directed towards improving system usability, rather than making assumptions about users' knowledge and self-efficacy, or blaming them for their lack thereof. On order to engage the technology adoption and retain users, and enjoy long-term positive effects, system developers should implement effective mechanisms for user control of data flows.

In our interviews, because we were asking participants detailed questions that essentially encouraged them to describe a complex view of what they would want in terms of data handling, they often came up with very specific distinctions between desirable and undesirable recipients, goals, locations, and circumstances. However, it is not clear whether consumers would use such fine-grained control mechanism, and whether such controls might be too complex to configure, and thus counterproductive in practice. In fact, at least one participant acknowledged explicitly that having the control she would want would render the system unusable:

> As far as putting what little business I have, like my bank account, on the computer, I would not be interested in that. *[I: Why?]* Because it's out of my control. I feel if you put it somewhere, it's out of my control. *[I: What if the system will give you control over the information, so you can decide who can access it, or if you don't want to share with anyone?]* That's just too much trouble. (P1)

Moreover, prior research has shown that users do not always take the full advantage of offered controls [20, 28, 40] and that such control is often illusory [57, 110].

However, this should not be interpreted as meaning such controls are not necessary. Indeed, it demonstrates the opposite: a necessity for better and more usable mechanisms for user controls. As our study and prior research shows, users in general, and older adults specifically, often lack understanding of the risks and awareness about the existing controls and risk protection/mitigation means [10, 23, 49, 51, 54], knowledge and skills about how to use those mechanisms [63, 70, 105, 119, 122], and declining cognitive and physical abilities to actually use them [56, 114]. Moreover, even commonly used mechanisms, such as passwords [42, 100, 107], ad-blockers [52, 96], and notices and warning messages [44, 46, 55, 99, 103], demonstrate a lack of usability, and are not always effective in their default configuration, and therefore require improvement.

Our participants also often expressed frustration about other usability aspects of current control mechanisms (see §6.6.6). Settings interfaces often use unintuitive labels and are hard to find [details in 49]. On the other hand, simplifying the process down to a one-time click-to-consent Terms of

Service + Privacy Policy while providing insufficient details [24]—or so many details as to render the documents unreadable (especially in combination with advanced legal language) [77]—is viewed by many users as completely inadequate.

The challenge for designers is therefore to provide sufficient specificity without making the controls too complicated and unusable. Elements of data handling that might be subject to user control include collection, further sharing, storage, processing and use, and protection from (other) privacy and security risks. In theory, a user might be able to control all the factors associated with the methods and policies of data management outlined in §6.2 and §6.6, such as ability to initiate, allow, deny, and limit the duration and frequency of collection and further sharing of data, including by specific data type, format, level of granularity, recipient (including primary, secondary, etc.), purpose, and more. It could also include the ability to modify the collected data (i.e. add, edit, delete, and limit the retention of stored data).

Due to the qualitative nature of our analysis and insufficient sample size for quantifying the prevalence and importance, we do not provide specific recommendations regarding what factors or sub-factors user controls should prioritise. Future empirical research and experimentation is required to design and test the optimal mechanisms of control.

7.2.2 Implications for policy and consumer protection. Data transparency and control can be voluntarily instituted by technology developers and device manufacturers, but also enforced via policy and legislation. In addition, encouraging designers' efforts to increase usability could be accomplished by enforcing adherence to industry standards and guidelines, and sanctioning systems that did not provide the adequate level of usability in their data privacy control mechanisms. The benchmark for such legal enforcement is the current requirement to provide the adequate level of security protection for the collected data, and the direct impact of the level of protection on the fine that the company will have to pay in case of data breach.

In addition to usability, *meaningful* transparency and control includes responsiveness to the full range of consumers' concerns. Legal protections are currently stronger for certain data types and subjects (for example, Health Insurance Portability and Accountability Act (HIPAA) and Right to Financial Privacy Act focus on medical and financial data protections respectively, The Children's Online Privacy Protection Act (COPPA) focuses on children's data). However, in order to address users' concerns privacy regulations need to be broader and to be able to adapt to the arising threats posed by advances in technology.

Although participants commonly cited concerns about sharing social security numbers and financial and medical records—paradigm examples of sensitive data (see §5)—they did not recall many instances of such data being actually misused. This may be the effect of stronger regulatory protections that, on the one hand, discourage attacks on such data, and, on the other hand, signal to the users the importance of protecting and be cautious with sharing of such data. For instance, one potential explanation is that participants believe information that tends to be perceived as sensitive and risky to share, is more likely to be protected by laws and treated with care by companies and organizations that have control of it, reducing the likelihood of violations (cf. [72]):

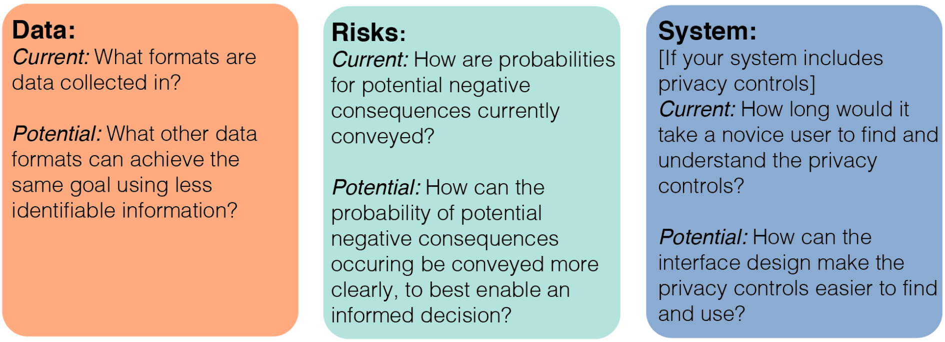
> I don't see [medical records] being so private. I know it is. I know lawsuits are the reason and so they have to be so so so so careful. (P123)

In contrast, participants believed that personal contact details, location, and browsing history—which most did not consider to be as sensitive in most contexts, but often were still not comfortable sharing—are frequently collected, shared with third parties, and misused. While participants were of course concerned about hacking and malicious attacks, many expressed more specific discomfort and feeling of invasion in response to very common (and often not illegal) business information practices such as consumer profiling and ad targeting (see §6.5 and Frik et al. 2019 [49]).

7.2.3 Future work: Guidelines and resources for assessment. We plan to use our model as the basis for a set of guidelines and actionable tools for researchers, policy makers, system designers, and educators, aimed at evaluating users' willingness to allow collection, sharing, and use of personal data. For instance, we will provide a list of validated scales—and, where missing, our suggestions—for evaluating the factors outlined in our model (e.g. privacy and security attitudes indices [43, 71], security behaviors intentions [41], usability evaluation methods [59], privacy self-efficacy [5, 27, 65] etc.).

We will also provide a directory of resources summarizing accumulated theoretical knowledge and empirical evidence about the impact of the model factors on users' privacy perceptions and willingness to share information.

7.2.4 Future work: Tools for designers/developers. We plan to develop and field-test a series of prompts, for example in the form of cards, to be used in brainstorming sessions, workshops, and assessments of product prototypes, by designers and developers of collaborative platforms that involve data collection and sharing (cf. [30, 48, 115]). Such prompts could help designers and developers think through how their users might assess the current privacy and security of their platforms, and react to different design choices, and challenge designers to think how existing systems can be modified to improve usability, safety, and privacy. Outside of industry, prompts could be used in research and in class activities.



Data:
Current: What formats are data collected in?

Potential: What other data formats can achieve the same goal using less identifiable information?

Risks:
Current: How are probabilities for potential negative consequences currently conveyed?

Potential: How can the probability of potential negative consequences occuring be conveyed more clearly, to best enable an informed decision?

System:
[If your system includes privacy controls]
Current: How long would it take a novice user to find and understand the privacy controls?

Potential: How can the interface design make the privacy controls easier to find and use?

Fig. 3. Examples of design prompts, as cards.

For instance, prompts such as those in Figure 3 could encourage designers to think about how the sensors currently embedded in the system will affect the amount, extent, and identifiability of collected information, and how the same goal can be achieved using less invasive approaches. In the Risk dimension, prompts can question how the risk probabilities are currently conveyed to the users and challenge the designers to think about better ways to convey that information. In the Systems dimension, the prompts can ask designers to assess the current availability and usability of privacy controls, and then encourage to propose more effective solutions. Additional prompts might include questions about how a user's propensity to share information would be different if they were inexperienced with the Internet, or if they had recently read about a data breach which affected millions of users.

By answering "as-is" questions regarding two or more systems or their prototypes, designers will be able to compare those systems or prototypes along the dimensions/factors/sub-factors in our model. For instance, designers will be able to compare which prototype of the system collects less identifiable information, offers easier to use interface design enabling users to control data flows, that requires lower levels of technology self-efficacy.

Moreover, the factors in our model may provide useful guidance not only in designing contextually-congruent sharing settings, but also in selecting features for training machine learning algorithms (e.g., similar to SPISM [18]) that would automate the prediction of personalised defaults, and help improve usability by reducing users' burden in configuring information-sharing settings, meet users' context-dependent preferences, and improve their overall information sharing experience.

7.2.5 Future work: Consumer education. Many elements in our model revealed the importance and opportunity for consumer education, for example, in order to improve their understanding of sharing scenarios, technology self-efficacy, align privacy expectations with the reality, educating about potential privacy and security risks, and ways to mitigate and protect against them.

In our future work, we plan to test whether the resources aimed at teaching privacy to a mass audience (such as Surveillance Self-Defense developed by the Electronic Frontier Foundation,[6] or Teaching Privacy[7]) are effective for the older population of users. We also plan to develop and test a curriculum for teaching best security and privacy practices geared specifically to older adults. We will customise the educational materials to better address the specific needs and concerns observed in our and prior work, provide verified information regarding the factors that affect their information-sharing decision making (e.g., probabilities and consequences of security risks), and will improve the accessibility of the materials to better cater to the cognitive and physical abilities of the elderly.

Additionally, in our future work we plan to estimate the gap in comprehension and familiarity with privacy and security vocabulary among older adults and younger population. For instance, we will test whether the language used in privacy policies, disclosures, and notices adequately conveys the information about information recipients, potential risks, their probabilities, and consequences, about potential inferences from the collected data, data retention and hosting policies, and involvement of humans in the data processing. Then we will ask respondents to propose the alternative terms to describe those aspects, which would make it more clear for them. Finally, we will map the used and proposed terms and develop guidance on how to improve transparency and effective communication about privacy and security between technologists and lawyers who design policies and interfaces and different socio-demographic groups of users, along the factors and sub-factors outlined in the model. By supporting seniors' learning of common terminology, we could also engage them in conversation about concerns, and prepare them to deal with tech support agents, chat bots, or systems' privacy policies and settings.

8 CONCLUSION

Our research aims at connecting disparate theoretical frameworks and scattered empirical evidence into a comprehensive model of information-sharing decision making.

Based on interviews with 46 participants aged 65+, we analyse their perspectives on information-sharing. We then develop a model of contextual factors that affect older adults' decision-making about collection, transmission, storage, sharing, and use of their personal information. Our qualitative model is more comprehensive and specific than prior theoretical and empirical studies, which each focus on a subset of factors. Moreover, it is based on empirical data that covers a wide range of technologies at once, from smartphones, laptops, and tablets to care robots, smart home devices, wearables, and Virtual Reality devices.

Older adults can be considered "extreme users" of modern technologies, whose needs and ability limitations are amplified with respect to more general population. Therefore, studying the privacy decision-making processes of elderly people, including non-users, will help us to understand the

[6] https://ssd.eff.org/
[7] https://teachingprivacy.org/

concerns surrounding emerging technologies across more general populations, and discover deeper insights that may be overlooked in the studies with typical user communities. Future research is called for to test whether the model is valid for other specific user groups and general population as well.

We also suggest practical implications of the proposed decision-making model for designing collaborative systems involving exchange of older adults' personal information, and propose concrete supports to aid in improving the design of such systems.

ACKNOWLEDGMENTS

We thank Leysan Nurgalieva, Joyce Lee, and Jiwon Lee for their contributions to data collection and analysis. We also thank Florian Schaub and participants in the 2nd Symposium on the Applications of Contextual Integrity for comments on the model, and anonymous WEIS reviewers for suggestions about the paper.

This work was supported by the Center for Long-Term Cybersecurity at UC Berkeley, the U.S. National Security Agency, National Science Foundation grants CNS-1514211 and CNS-1528070, and the Rose Foundation for Communities and the Environment.

REFERENCES

[1] Mark S Ackerman, Lorrie Faith Cranor, and Joseph Reagle. 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*. ACM, 1–8.

[2] Alessandro Acquisti, Leslie K John, and George Loewenstein. 2013. What is privacy worth? *The Journal of Legal Studies* 42, 2 (2013), 249–274.

[3] Anne Adams. 2000. Multimedia information changes the whole privacy ballgame. In *Proceedings of the tenth conference on Computers, freedom and privacy: challenging the assumptions*. ACM, 25–32.

[4] Icek Ajzen et al. 1991. The theory of planned behavior. *Organizational behavior and human decision processes* 50, 2 (1991), 179–211.

[5] Syed H Akhter. 2014. Privacy concern and online transactions: the impact of internet self-efficacy and internet involvement. *Journal of Consumer Marketing* (2014).

[6] Abdulmajeed Alqhatani and Heather Richter Lipford. 2019. "There is nothing that I need to keep secret": Sharing Practices and Concerns of Wearable Fitness Data. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association. https://www.usenix.org/conference/soups2019/presentation/alqhatani

[7] Irwin Altmacbi. 1977. Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues* 33, 3 (1977), 66–84.

[8] Irwin Altman. 1975. The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. (1975).

[9] Bonnie Anderson, Tony Vance, Brock Kirwan, David Eargle, and Seth Howard. 2014. Users aren't (necessarily) lazy: Using neurois to explain habituation to security warnings. (2014).

[10] Keith B Anderson. 2004. *Consumer fraud in the United States: An FTC survey.* Federal Trade Commission.

[11] Monica Anderson. 2015. Smartphone, computer or tablet? 36% of Americans own all three. *Pew Research Center* (2015).

[12] Noah Apthorpe, Yan Shvartzshnaider, Arunesh Mathur, Dillon Reisman, and Nick Feamster. 2018. Discovering smart home Internet of Things privacy norms using contextual integrity. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 2 (2018), 59.

[13] Kenneth A Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On, and Irwin Reyes. 2020. Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps. *Berkeley Technology Law Journal* 35 (2020).

[14] Adam Barth, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. 2006. Privacy and contextual integrity: Framework and applications. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP.2006.32

[15] Martin W Bauer, George Gaskell, and Nicholas C Allum. 2000. Quality, quantity and knowledge interests: Avoiding confusions. *Qualitative researching with text, image and sound: A practical handbook* (2000), 3–17.

[16] Scott Beach, Richard Schulz, Julie Downs, Judith Matthews, Bruce Barron, and Katherine Seelman. 2009. Disability, age, and informational privacy attitudes in quality of life technology applications: Results from a national web survey. *ACM Transactions on Accessible Computing (TACCESS)* 2, 1 (2009), 5.

[17] Sebastian Benthall. 2019. Situated Information Flow Theory. In *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (HotSoS '19)*. Association for Computing Machinery, New York, NY, USA, Article Article 5, 10 pages. https://doi.org/10.1145/3314058.3314066

[18] Igor Bilogrevic, Kévin Huguenin, Berker Agir, Murtuza Jadliwala, and Jean-Pierre Hubaux. 2013. Adaptive information-sharing for privacy-aware mobile social networks. In *Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing*. 657–666.

[19] L Boise, K Wild, N Mattek, M Ruhl, HH Dodge, and J Kaye. 2013. Willingness of older adults to share data and privacy concerns after exposure to unobtrusive in-home monitoring. *Gerontechnology: International Journal on the Fundamental Aspects of Technology to Serve the Ageing Society* (2013).

[20] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4, 3 (2013), 340–347.

[21] Virginia Braun and Victoria Clarke. 2013. *Successful qualitative research: A practical guide for beginners.* sage.

[22] Paula Bruening and Heather Patterson. 2016. A Context-Driven Rethink of the Fair Information Practice Principles. (23 September 2016). Retrieved 27 May, 2020 from https://ssrn.com/abstract=2843315

[23] Jean Camp and Kay Connelly. 2008. Beyond consent: Privacy in ubiquitous computing (Ubicomp). *Digital Privacy: Theory, Technologies, and Practices* (2008), 327–343.

[24] Eoin Carolan. 2016. The continuing problems with online consent under the EU's emerging data protection principles. *Computer Law & Security Review* 32, 3 (2016), 462–473.

[25] BD Carpenter and S Buday. 2007. Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior* (2007).

[26] Rajarshi Chakraborty, Claire Vishik, and H Raghav Rao. 2013. Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems* 55, 4 (2013), 948–956.

[27] Hsuan-Ting Chen and Wenhong Chen. 2015. Couldn't or wouldn't? The influence of privacy concerns and self-efficacy in privacy management on privacy protection. *Cyberpsychology, Behavior, and Social Networking* 18, 1 (2015), 13–19.

[28] Emily Christofides, Amy Muise, and Serge Desmarais. 2009. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology & behavior* 12, 3 (2009), 341–345.

[29] Jane Chung, George Demiris, and Hilaire Thompson. 2016. Ethical Considerations Regarding the Use of Smart Home Technologies for Older Adults: An Integrative Review. *Annual Review of Nursing Research* 34 (2016), 155–181.

[30] J Cleland-Huang, T Denning, T Kohno, F Shull, and S Weber. 2016. Keeping Ahead of Our Adversaries. *IEEE Software* 33, 3 (2016), 24–28.

[31] Caitlin D Cottrill et al. 2015. Location privacy preferences: A survey-based analysis of consumer awareness, trade-off, and decision-making. *Transportation Research Part C: Emerging Technologies* 56 (2015), 132–148.

[32] JF Coughlin, LA D'Ambrosio, B Reimer, and MR Pratt. 2007. Older adult perceptions of smart home technologies: implications for research, policy market innovations in healthcare. *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (2007).

[33] KL Courtney, G Demeris, M Rantz, and M Skubic. 2008. Needing smart home technologies: the perspectives of older adults in continuing care retirement communities. *Informatics in Primary Care* (2008).

[34] Lynne Coventry and Pam Briggs. 2016. Mobile Technology for Older Adults: Protector, Motivator or Threat?. In *Human Aspects of IT for the Aged Population: Design for Aging*, Jia Zhou and Gavriel Salvendy (Eds.). Springer International Publishing, Cham, 424–434.

[35] Sara J Czaja, Wendy A Rogers, Arthur D Fisk, Neil Charness, and Joseph Sharit. 2009. *Designing for Older Adults: Principles and Creative Human Factors Approaches.* CRC Press.

[36] George Demiris, Brian K Hensel, Marjorie Skubic, and Marilyn Rantz. 2008. Senior residents' perceived need of and preferences for "smart home" sensor technologies. *International journal of technology assessment in health care* 24, 1 (2008), 120–124.

[37] G Demiris, MJ Rantz, MA Aud, KD Marek, HW Tyrer, M Skubic, and AA Hussam. 2004. Older adults' attitudes towards and perceptions of 'smart home' technologies: a pilot study. *Medical Informatics and the Internet in Medicine* (2004).

[38] Tamara Dinev, Valentina Albano, Heng Xu, Alessandro D'Atri, and Paul Hart. 2016. *Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective.* Springer International Publishing, Cham, 19–50.

[39] Tamara Dinev and Paul Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research* 17, 1 (2006), 61–80.

[40] Serge Egelman, Andrew Oates, and Shriram Krishnamurthi. 2011. Oops, I did it again: mitigating repeated access control errors on facebook. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems.* 2295–2304.

[41] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems.* 2873–2882.

[42] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* ACM, 2379–2388.

[43] Cori Faklaris, Laura A Dabbish, and Jason I Hong. 2019. A self-report measure of end-user security attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019).*

[44] Adrienne Porter Felt, Serge Egelman, Matthew Finifter, Devdatta Akhawe, and David Wagner. 2012. How to ask for permission. In *Proceedings of the 7th USENIX conference on Hot Topics in Security (HotSec'12)*. USENIX Association, Berkeley, CA, USA, 7–7. http://dl.acm.org/citation.cfm?id=2372387.2372394

[45] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.

[46] Adrienne Porter Felt, Robert W. Reeder, Hazim Almuhimedi, and Sunny Consolvo. 2014. Experimenting at Scale with Google Chrome's SSL Warning. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 2667–2670. https://doi.org/10.1145/2556288.2557292

[47] Martin Fishbein and Icek Ajzen. 2011. *Predicting and changing behavior: The reasoned action approach.* Psychology press.

[48] B Friedman and D Hendry. 2012. The Envisioning Cards: A Toolkit for Catalyzing Humanistic and Technical Imaginations. Association for Computing Machinery, New York, NY, USA.

[49] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS '19)*. USENIX.

[50] Vaibhav Garg, L Jean Camp, Katherine Connelly, Kalpana Shankar, and Lesa Mae Lorenzen-Huber. 2011. Privacy Framework for Older Adults. In *Workshop on Security and Human Behavior, Pittsburgh, PA*.

[51] V. Garg, L. Lorenzen-Huber, L. J. Camp, and K. Connelly. 2012. Risk Communication Design for Older Adults. *Gerontechnology* 11, 2 (2012), 166–173.

[52] Arthur Gervais, Alexandros Filios, Vincent Lenders, and Srdjan Capkun. 2017. Quantifying web adblocker privacy. In *European Symposium on Research in Computer Security*. 21–42.

[53] Stacey Gray. 2016. *Always On: Privacy Implications of Microphone-Enabled Devices.* Technical Report. Future of Privacy Forum. https://www.ftc.gov/system/files/documents/public_comments/2016/08/00003-128652.pdf

[54] Galen A Grimes, Michelle G Hough, Elizabeth Mazur, and Margaret L Signorella. 2010. Older adults' knowledge of Internet hazards. *Educational Gerontology* 36, 3 (2010), 173–192.

[55] Marian Harbach, Markus Hettig, Susanne Weber, and Matthew Smith. 2014. Using Personal Examples to Improve Risk Communication for Security and Privacy Decisions. In *Proceedings of the 2014 CHI Conference on Human FActors in Computing Systems (CHI'14)*. ACM, New York, NY, USA, 2647–2656. https://doi.org/10.1145/2556288.2556978

[56] Eszter Hargittai and Kerry Dobransky. 2017. Old Dogs, New Clicks: Digital Inequality in Skills and Uses among Older Adults. *Canadian Journal of Communication* 42, 2 (2017). https://cjc-online.ca/index.php/journal/article/view/3176/3351

[57] Christopher M Hoadley, Heng Xu, Joey J Lee, and Mary Beth Rosson. 2010. Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications* 9, 1 (2010), 50–60.

[58] Leslie K John, Alessandro Acquisti, and George Loewenstein. 2010. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research* 37, 5 (2010), 858–873.

[59] Ronald Kainda, Ivan Flechais, and AW Roscoe. 2010. Security and usability: Analysis and evaluation. In *2010 International Conference on Availability, Reliability and Security*. IEEE, 275–282.

[60] HG Kang, DF Mahoney, H Hoenig, VA Hirth, P Bonato, I Hajjar, and LA Lipsitz. 2010. In situ monitoring of health in older adults: technologies and issues. *Journal of the American Geriatrics Society* (2010).

[61] Omead Kohanteb, Owen Tong, Heidi Yang, Thidanun Saensuksopa, and Saba Kazi. 2015. *Guidelines for Designing Connected Devices.* Technical Report. Carnegie Mellon University. http://signifiers.io/signifiers/guidelines.html Accessed on 26 February 2018.

[62] Josephine Lau, Benjamin Zimmerman, and Florian Schaub. 2018. Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 102.

[63] SG Ledbetter and L Choi-Allum. 2005. *Perspectives Past, Present, and Future: Traditional and Alternative Financial Practices of the 45+ Community.* Technical Report. AARP. https://assets.aarp.org/rgcenter/general/2004_perspectives.pdf Accessed 2 May 2019.

[64] Scott Lederer, Jennifer Mankoff, and Anind K Dey. 2003. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI'03 extended abstracts on Human factors in computing systems*. ACM, 724–725.

[65] Hyun-Hwa Lee and Jessica T Hill. 2013. Moderating effect of privacy self-efficacy on location-based mobile marketing. *International Journal of Mobile Communications* 11, 4 (2013), 330–350.

[66] Linda Lee, Joong Hwa Lee, Serge Egelman, and David Wagner. 2016. Information disclosure concerns in the age of wearable computing. In *Proceedings of the NDSS Workshop on Usable Security (USEC '16)*. Internet Society. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/

information-disclosure-concerns-in-the-age-of-wearable-computing.pdf

[67] Huigang Liang and Yajiong Xue. 2009. Avoidance of Information Technology Threats: A Theoretical Perspective. *MIS Quarterly* 33, 1 (2009), 71–90. http://www.jstor.org/stable/20650279

[68] Lili Liu, Eleni Stroulia, Ioanis Nikolaidis, Antonio Miguel-Cruz, and Adriana Rios Rincon. 2016. Smart homes and home health monitoring technologies for older adults: A systematic review. *International journal of medical informatics* 91 (2016), 44–59.

[69] L Lorenzen-Huber, M Boutain, LJ Camp, K Shankar, and KH Connelly. 2011. Privacy, technology, and aging: A proposed framework. *Ageing International* (2011).

[70] Mary Madden and Lee Rainie. 2015. *Americans' Attitudes About Privacy, Security, and Surveillance.* Technical Report. Pew Research Center. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ Accessed on 30 May 2019.

[71] Naresh K. Malhotra, Sung S. Kim, and James Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, The Scale, and A Causal Model. *Information Systems Research* 15, 4 (December 2004), 336–355.

[72] Nathan Malkin, Julia Bernd, Maritza Johnson, and Serge Egelman. 2018. 'What *can't* data be used for?' Privacy expectations about smart TVs in the U.S.. In *Proceedings of the 3rd European Workshop on Usable Security (EuroUSEC), London, UK, April 23, 2018.*

[73] Nathan Malkin, Joe Deatrick, Allen Tong, Primal Wijesekera, Serge Egelman, and David Wagner. 2019. Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies* 2019, 4 (2019), 250–271.

[74] Kirsten Martin and Katie Shilton. 2016. Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society* 32, 3 (2016), 200–216.

[75] Marifran Mattson and Maria Brann. 2002. Managed care and the paradox of patient confidentiality: A case study analysis from a communication boundary management perspective. *Communication Studies* 53, 4 (2002), 337–357. https://doi.org/10.1080/10510970209388597

[76] Faith McCreary, Alexandra Zafiroglu, and Heather Patterson. 2016. The contextual complexity of privacy in smart homes and smart buildings. In *International Conference on HCI in Business, Government, and Organizations.* Springer, 67–78.

[77] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *Isjlp* 4 (2008), 543.

[78] Andrew McNeill, Pam Briggs, Jake Pywell, and Lynne Coventry. 2017. Functional privacy concerns of older adults about pervasive health-monitoring systems. In *Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments.* ACM, 96–102.

[79] Maya Meinert. 2018. Seniors will soon outnumber children, but the U.S. isn't ready. (21 June 2018). Retrieved March 28, 2019 from https://news.usc.edu/143675/aging-u-s-population-unique-health-challenges/

[80] Anita Melander-Wikman, Ylva Fältholm, and Gunvor Gard. 2008. Safety vs. Privacy: Elderly Persons' Experiences of a Mobile Safety Alarm. *Health & Social Care in the Community* 16 (2008), 337–46.

[81] AS Melenhorst, WA Rogers, and DG Bouwhuis. 2006. Older adults' motivated choice for technological innovation: Evidence for benefit-driven selectivity. *Psychology and aging* (2006).

[82] TL Mitzner, JB Boron, CB Fausset, AE Adams, N Charness, SJ Czaja, K Dijkstra, AD Fisk, WA Rogers, and J Sharit. 2010. Older adults talk technology: Technology usage and attitudes. *Computers in Human Behavior* (2010).

[83] Alessandro Montanari, Afra Mashhadi, Akhil Mathur, and Fahim Kawsar. 2016. Understanding the Privacy Design Space for Personal Connected Objects. In *Proceedings of the 30th International BCS Human Computer Interaction Conference: Fusion! (HCI '16).* BCS Learning & Development Ltd., Swindon, UK, Article 18, 18:1–18:13 pages. https://doi.org/10.14236/ewic/HCI2016.18

[84] Elizabeth D Mynatt, A-S Melenhorst, A-D Fisk, and Wendy A Rogers. 2004. Aware technologies for aging in place: understanding user needs and attitudes. *IEEE Pervasive Computing* 3, 2 (2004), 36–41.

[85] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017).* USENIX Association, Santa Clara, CA, 399–412. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

[86] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The Influence of Friends and Experts on Privacy Decision Making in IoT Scenarios. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 48.

[87] Helen Nissenbaum. 2004. Privacy as Contextual Integrity. *Washington Law Review* 79, 119 (2004), 101–139.

[88] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

[89] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (Fall 2011), 32–48.

[90] Leysan Nurgalieva, Alisa Frik, Francesco Ceschel, Serge Egelman, and Maurizio Marchese. 2019. Information design in an aged care context: Views of older adults on information sharing in a care triad. In *Proceedings of the 13th EAI*

International Conference on Pervasive Computing Technologies for Healthcare. 101–110.

[91] Leysia Palen and Paul Dourish. [n. d.]. Unpacking "Privacy" for a Networked World. In *Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (CHI '03)*.

[92] Sandra Petronio. 1991. Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory* 1, 4 (1991), 311–335.

[93] Sandra Petronio. 2013. Brief Status Report on Communication Privacy Management Theory. *Journal of Family Communication* 13, 1 (2013), 6–14. https://doi.org/10.1080/15267431.2013.743426

[94] Richard E Petty and John T Cacioppo. 1986. The elaboration likelihood model of persuasion. In *Communication and persuasion*. Springer, 1–24.

[95] Matthew D Pickard, Catherine A Roster, and Yixing Chen. 2016. Revealing sensitive information in personal interviews: Is self-disclosure easier with humans or avatars and under what conditions? *Computers in Human Behavior* 65 (2016), 23–30.

[96] Enric Pujol, Oliver Hohlfeld, and Anja Feldmann. 2015. Annoyed users: Ads and ad-block usage in the wild. In *Proceedings of the Internet Measurement Conference*. 93–106.

[97] Yonglin Ren, Richard Werner, Nelem Pazzi, and Azzedine Boukerche. 2010. Monitoring patients via a secure and mobile healthcare system. *IEEE Wireless Communications* 17, 1 (2010), 59–65.

[98] R.W. Rogers and S. Prentice-Dunn. 1997. *Protection Motivation Theory*. Plenum Press.

[99] Florian Schaub, Rebecca Balebako, and Lorrie Faith Cranor. 2017. Designing Effective Privacy Notices and Controls. *IEEE Internet Computing* 21, 3 (2017), 70–77.

[100] Richard Shay, Patrick Gage Kelley, Saranga Komanduri, Michelle L Mazurek, Blase Ur, Timothy Vidas, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2012. Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *Proceedings of the eighth symposium on usable privacy and security*. ACM, 7.

[101] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein. 1977. Behavioral decision theory. *Annual review of psychology* 28, 1 (1977), 1–39.

[102] Frederic Stutzman and Woodrow Hartzog. 2012. Boundary Regulation in Social Media. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW '12)*. ACM, New York, NY, USA, 769–778. https://doi.org/10.1145/2145204.2145320

[103] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying wolf: an empirical study of SSL warning effectiveness. In *Proceedings of the 18th USENIX Security Symposium (SSYM'09)*. USENIX Association, Berkeley, CA, USA, 399–416. http://dl.acm.org/citation.cfm?id=1855768.1855793

[104] Madiha Tabassum, Tomasz Kosiński, Alisa Frik, Nathan Malkin, Primal Wijesekera, Serge Egelman, and Heather Richter Lipford. 2019. Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3, 4 (2019), 1–23.

[105] Jiang Tao and Hu Shuijing. 2016. The Elderly and the Big Data: How Older Adults Deal with Digital Privacy. In *2016 International Conference on Intelligent Transportation, Big Data, & Smart City*. IEEE, 285–288.

[106] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22, 2 (2011), 254–268.

[107] Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, et al. 2012. How does your password measure up? The effect of strength meters on password creation.. In *USENIX Security Symposium*. 65–80.

[108] US Census Bureau. 2018. Older People Projected to Outnumber Children for First Time in U.S. History. (13 March 2018). Retrieved March 28, 2019 from https://www.census.gov/newsroom/press-releases/2018/cb18-41-population-projections.html Release CB18-41.

[109] Anthony Vance, David Eargle, Jeffrey L Jenkins, C Brock Kirwan, and Bonnie Brinton Anderson. 2019. The fog of warnings: how non-essential notifications blur with security warnings. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*.

[110] Na Wang, Heng Xu, and Jens Grossklags. 2011. Third-party apps on Facebook: privacy and the illusion of control. In *Proceedings of the 5th ACM symposium on computer human interaction for management of information technology*. 1–10.

[111] Jason Wiese, Patrick Gage Kelley, Lorrie Faith Cranor, Laura Dabbish, Jason I Hong, and John Zimmerman. 2011. Are you close with me? Are you nearby? Investigating social groups, closeness, and willingness to share. In *Proceedings of the 13th international conference on Ubiquitous computing*. 197–206.

[112] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android permissions remystified: A field study on contextual integrity. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*. 499–514.

[113] Katherine Wild, Linda Boise, Jay Lundell, and Anna Foucek. 2008. Unobtrusive in-home monitoring of cognitive and physical health: Reactions and perceptions of older adults. *Journal of applied gerontology* 27, 2 (2008), 181–200.

[114] Sherry L Willis, K Warner Schaie, and Mike Martin. 2009. Cognitive plasticity. In *Handbook of Theories of Aging*. Springer, 295–322.

[115] RY Wong, DK Mulligan, E Van Wyk, J Pierce, and J Chuang. 2017. Eliciting Values Reflections by Engaging Privacy Futures Using Design Workbooks. *Proceedings of the ACM on Human–Computer Interaction* 1, CSCW, Article 111 (Dec. 2017), 26 pages.

[116] F Xing, G Peng, T Liang, and J Jiang. 2018. Challenges for Deploying IoT Wearable Medical Devices Among the Ageing Population. *International Conference on Distributed, Ambient, and Pervasive Interactions* (2018).

[117] Mu Yang, Yijun Yu, Arosha K Bandara, and Bashar Nuseibeh. 2014. Adaptive sharing for online social networks: A trade-off between privacy risk and social benefit. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 45–52.

[118] Lucy Yardley. 2000. Dilemmas in qualitative health research. *Psychology and health* 15, 2 (2000), 215–228.

[119] Eva-Maria Zeissig, Chantal Lidynia, Luisa Vervier, Andera Gadeib, and Martina Ziefle. 2017. Online privacy perceptions of older adults. In *International Conference on Human Aspects of IT for the Aged Population*. Springer, 181–200.

[120] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*. 65–80.

[121] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX, Santa Clara, CA, 65–80. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[122] Kathryn Zickuhr and Mary Madden. 2012. *Older adults and Internet use*. Technical Report. Pew Internet & American Life Project.

A CONTEXTUAL INFORMATION-SHARING DECISION-MAKING MODEL.

DECISION MAKER

- (a) **Attitudes towards privacy** (§6.1.1)
    - (i) Circumstances that make the decision maker feel especially vulnerable to certain risks
    - (ii) Personal experiences with privacy or security violations
    - (iii) *Decision Maker > Privacy expectations*
- (b) **Privacy expectations** (§6.1.2)
    - (i) Decision maker's perception of their own ability to understand the data sharing scenario/consequences
        - Knowledge of the specific data flows and mechanisms involved
        - Past experiences with similar or related data sharing scenarios (including benefits and risks)
    - (ii) *Environment > Norms about appropriate or usual behavior*
    - (iii) *Environment > Norms about appropriate or usual information sharing*
    - (iv) *Environment > Laws and regulations about information sharing*
    - (v) *Environment > Stories*
- (c) **Technology acceptance** (§6.1.3)
    - (i) Technology self-efficacy
        - *Decision Maker > Privacy expectations > Understanding of the sharing scenario*
    - (ii) Circumstances that increase the need to share certain information
- (d) **Desire for agency and control** (§6.1.4)

DATA

- (a) **Relevance to the recipient/goal** (§6.2.1)
- (b) **Requirement for data** (§6.2.2)
- (c) **Amount or extent** (§6.2.3)
    - (i) Accumulation of data over time
        - Continuity of data collection
        - *System > Data retention policies*
    - (ii) Granularity and specificity of the data
    - (iii) The format of the data or the type of sensor
- (d) **Accuracy** (§6.2.4)

RECIPIENTS

- (a) **Trust in recipients** (§6.3.1)
    - (i) Evaluation of recipients' legitimacy and (general) intentions)
        - Past experiences within the relationship
        - Recipients' reputation
            - *Environment > Stories*
        - Assessment based on appearances
    - (ii) Recipients' judgement and competence/ability
- (b) **Degree of removal** (§6.3.2)
- (c) **Recipients' potential reaction** (§6.3.3)
    - (i) Perceived desire to receive the information
    - (ii) Expected affective reaction
        - *Environment > Norms about appropriate or usual behavior*
        - *Environment > Norms about appropriate or usual information sharing*
    - (iii) Likeliness that the recipient already knows or could easily guess the information

PURPOSES AND BENEFITS

- (a) **Who benefits accrue to** (§6.4.1)
- (b) **Perceived likelihood of benefits occurring** (§6.4.2)
    - (i) *Data > Technology acceptance*
    - (ii) *Data > Relevance to the recipient/goal*
    - (iii) *Recipient > Trust in recipient*
- (c) **Extent of benefits** (§6.4.3)
    - (i) Importance or added value for the party who accrues the benefit
    - (ii) Urgency or time sensitivity of receiving the benefit

RISKS

- (a) **Perceived likelihood of negative consequences** (§6.5.1)
  - (i) Assessment of whether the recipient's primary or secondary purposes carry risks
    - Expected material value of the data to the recipient
    - *Recipient > Trust in recipients*
    - *System > Data retention*
    - *Environment > Laws and regulations about information sharing*
  - (ii) Assessment of the potential for risks unrelated to the recipient's purposes
    - *System > Connection to the Internet*
    - *Environment > Stories*
  - (iii) Potential inferences from the data
  - (iv) Reusability of the data across contexts
  - (v) *Data > Amount or extent*
  - (vi) *System > Ability to control data flows and protect against or mitigate risks*
- (b) **Potential severity of consequences** (§6.5.2)
- (c) **Who accrues the consequences** (§6.5.3)

SYSTEM

- (a) **Decision maker's experience of sharing** (§6.6.1)
  - (i) Intrusiveness of the data collection practices
  - (ii) Usability of the system
  - (iii) *Decision Maker > Technology acceptance > Technology self-efficacy*
- (b) **Data retention** (§6.6.2)
- (c) **Connection to the Internet Transmission channel** (§6.6.3)
- (d) **Human involvement** (§6.6.4)
- (e) **Transparency about data flows** (§6.6.5)
- (f) **Ability to control data flows and mitigate and protect against risks** (§6.6.6)
  - (i) Existence and availability of relevant means of control/protection/mitigation
  - (ii) Cost of control, protection, mitigation
    - Monetary cost
    - Required time and effort
      - – *Decision maker > Technology acceptance > Technology self-efficacy*
  - (iii) Likely effectiveness of the means of control/protection/mitigation

ENVIRONMENT

- (a) **Norms about appropriate or usual behavior** (§??)
  - (i) Behavioral norms within a specific small group/community
  - (ii) Broader social norms of behavior
  - (iii) Laws about behavior
- (b) **Norms about appropriate or usual information sharing** (§6.7.2)
  - (i) Information-sharing norms within a specific small group/community
  - (ii) Broader social norms about information sharing
- (c) **Laws and regulations about information sharing** (§6.7.3)
- (d) **Stories about information sharing** (§6.7.4)
  - (i) Current media stories
  - (ii) Past experiences of decision maker's close connections
- (e) **Alternative options for achieving the decision-maker's goal** (§6.7.5)
  - (i) Existence / availability of alternatives
  - (ii) Cost of alternatives
    - Monetary cost
    - Required time and effort
      - – *Decision maker > Technology acceptance > Technology self-efficacy*
  - (iii) Likely effectiveness of the alternatives
  - (iv) Preference for in-person communication