A Model of Contextual Factors Affecting Older Adults' Information-Sharing Decisions in the US

ALISA FRIK, International Computer Science Institute
JULIA BERND, International Computer Science Institute
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 and context that influence those decisions. 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. We develop a detailed model of the contextual factors that combine in complex ways to affect older adults' decision-making about information sharing. We 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.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; *Usability in security and privacy*; • **Social and professional topics →** *Seniors*; • **Human-centered computing → User models**.

Additional Key Words and Phrases: information sharing, data flows, interviews, contextual integrity

ACM Reference Format:
Alisa Frik, Julia Bernd, and Serge Egelman. 2022. A Model of Contextual Factors Affecting Older Adults' Information-Sharing Decisions in the US. *ACM Trans. Comput.-Hum. Interact.* , (June 2022), 48 pages.

1 INTRODUCTION

By 2030, 1 in 5 US residents is projected to reach the retirement age of 65 years or older [105]. The expansion of the population of older adults will bring additional challenges associated with addressing their everyday needs, including physical and mental health needs [70]. Information and communication technologies (ICT) can facilitate service provision and reduce the cost of care [74], 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 involved in care.

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

1073-0516/2022/6-ART
https://doi.org/

At the same time, design of such systems must account for the fact that older adults may have more difficulty understanding information flows and attendant risks, for example due to having less technological experience than other populations [22, 37, 42, 45, 47, 51, 117] or simply due to changes in cognitive or physical ability [48, 109]. Prior work has shown that older adults are less aware of privacy and security risks [8, 21, 45, 46, 49] and are less likely to protect themselves [53, 60, 103, 114, 117]. Thus, the benefits of transparency around data flows between older adults and caregivers should be protected through suitable security and privacy safeguards, assistance and technical support provided by more tech-savvy stewards and caregivers, and training of older adults to protect their online privacy and security independently [66, 67, 73, 77, 82, 94, 95].

Accounting for context is particularly important. For example, sharing information about medication allergies with a healthcare provider is different from sharing that one has had an abortion, both in terms of relevance to current care and potential risks of sharing. The recipient's use of the information also plays a role: using someone's medical information to assess what care they need would be more appropriate than describing it in a public blog post, or making fun of it with friends [cf. 86]. Failure to address privacy and security concerns [15, 23, 29, 34, 39, 89] and account for granular, context-dependent preferences about information sharing [20, 87, 93] may introduce barriers to adoption of ICT that could otherwise improve the level of cooperation and information sharing between elderly patients and their caregivers.

In this paper, we examine the following **research question**: What contextual factors drive older adults' decisions about whether to engage in information exchange? To answer this research question, we analyzed 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., 1, 3, 10, 50, 55, 56, 62, 65, 69, 79, 87, 96]. 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 when we examined them in terms of implicit underlying factors.

However, as we discuss in §2, prior work on what specific contextual factors affect information-sharing decision-making is still limited. In this paper, we aim to contribute to the literature about context in privacy, and expand the body of empirical work on this topic. The central contribution of this paper is in proposing a comprehensive model of factors affecting the context-specific decision-making of older adults about information sharing. The 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.

By comparing our qualitative interview findings 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, evaluate the relative impact of the factors on decision-making, 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 improving 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, which are scarce and disconnected, are incomplete due to focusing in-depth on specific dimensions of sharing decisions, or lack guidelines for practical application.

In addition, our findings have practical implications for technology development, education, and policy. 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, more privacy-respecting online ecosystem, while at the same time, educating consumers can inform their privacy expectations and improve their safety.

Organization. In §2, we begin by reviewing empirical studies of data sharing preferences and theoretical literature on privacy decision-making. 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 empirical evidence aiming at illustrating data sharing decisions of the general population and older adults in particular, then we review theoretical frameworks aiming at explaining and modeling such decisions.

2.1 Empirical Evidence

2.1.1 Data sharing preferences of the general population. There is a large body of work on users' privacy attitudes, preferences and expectations in different contexts, such as e-commerce scenarios, healthcare contexts, and smart homes [e.g. 2, 54, 97, 115]. Focusing on virtual reality, video conferencing, and Internet multicasting, Adams [4] developed a model of privacy factors—information receivers (mediated by trust), potential usage of collected data (affecting risk/benefit trade-offs), and information sensitivity—that affect users' perceptions of privacy in multimedia communications. He notes that other contextual factors may affect users' perceptions, but does not elaborate on what those factors are and how they impact perceptions.

Lederer et al. [54] evaluated the relative importance of two of the factors identified by Adams [4], recipient and context, on mobile communication privacy preferences. They found that recipients are stronger predictors of privacy decisions than disclosure context, and that users are more likely to disclose information to the same recipient in different contexts than to different recipients in the same context. However, they didn't explore why recipients have such a large impact, what other (potentially more impactful) aspects may constitute "context," and didn't examine the impact of other factors, found in prior work, such as risk/benefit trade-offs.

Focusing on IoT-related privacy concerns, Naeini et al. [80] surveyed over 1000 participants 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 surveys, Lee et al. [56] found that users are concerned about privacy and security risks associated with wearable technologies that collect or store financial information or video recordings. In contrast, with respect to fitness data specifically, Alqhatani and Lipford's [5] 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. A survey by Mehdy et al. [69] identified interactions between privacy attitudes and contextual details like information type, recipient role, and trust source in determining sharing decisions, but did not model a full suite of contextual factors. Naeini et al. [81] found that social cues, such as the data-sharing decisions of friends, can impact users' IoT privacy decisions. Wiese et al. [107] found that certain aspects of relationships between connections ('friends') on Facebook, such as frequency of communication and tie strength, affect users' decisions to share information with those connections in social media.

Bilogrevic et al. [16] 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 (e.g., 'person', including user's familiarity and social ties with the recipient), achieving 90% accuracy in predicting sharing decisions. Although prior research shows potential in predicting users' information sharing preferences and expectations, the accuracy of such systems depends on having well-grounded models of users' contextual decision-making. As we discuss in Section 2.2, current models don't adequately satisfy this need.

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 [13, 24, 40, 41, 44, 58, 59, 68, 108]. For instance, a perceived need for technology and lack of awareness of privacy risks have been shown to affect older adults' data sharing decisions [17, 59]. In focus groups with 64 older adults, Lorenzen-Huber et al. [59] found that their privacy concerns are negatively associated with perceived usefulness of in-home monitoring technologies to meet *current* needs, and positively associated with the perceived sensitivity and granularity of the data. They were also concerned that high granularity may increase the burden of caregiving, and wanted 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 recipients having a significant role. For instance, older adults have been shown to feel comfortable sharing data with their doctors [13, 108]. Boise et al. [17] found that 72% of older adults are willing to share data collected by healthmonitoring systems with caregivers and family members, but are concerned about unintended parties. Xing et al. [111] found that seniors and their family members were worried that health data collected by wearables would not be adequately protected and might therefore be subject to misuse. Mynatt et al. [78] 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).

In contrast, Anaraky et al. [44] found that older adults' information-sharing decision-making processes were less based on trust in recipients than younger adults', and more based on weighing risks and benefits. 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) [13, 52, 108]. Poor health conditions also make users more likely to accept the privacy trade-off. For example, Beach et al. [13] found that disabled adults were more willing to share their information compared to non-disabled adults. Courtney et al. [30] found that older adults' perceived need for a technology is likely to override their privacy preferences, consistent with prior findings on cost-benefit trade-offs. [52, 72, 74]

Nevertheless, a few research efforts have suggested that older adults' privacy concerns are potential barriers to technology adoption [23, 29, 34]. For instance, Demiris et al. [33], in focus groups with 14 seniors, found that older adults have privacy concerns that might affect their adoption of sensor-based smart home technologies, and demand features that allow them to access the sensor data and specify allowed recipients [33]. A meta-review on telehealth and telecare by Pool et al. [93] found that context-dependent concerns about specific aspects of data collection could affect older adults' adoption of those technologies. There is a need for suitable and adaptive cybersecurity safeguards that could ensure better online safety and security while preserving older adults' privacy and autonomy [27, 66, 77]. Such safeguards would also facilitate more substantively shared decision-making with caregivers [67, 73]. This body of research suggests that implementing user controls over information flows is vital for the market success of data-driven collaborative systems.

While the empirical work described above provides useful anecdotal evidence, it is fragmented, as every study explores only certain targeted factors in isolation, and each defines context differently (if at all). Lack of shared understanding of these factors and contexts, and lack of a theoretical foundation for the design of empirical studies, undermine researchers' ability to replicate these effects, draw generalizable conclusions, and make recommendations. Thus, there is a pressing need for theoretical frameworks to analyze information-sharing decision-making.

2.2 Theoretical Frameworks

In this section we review the most relevant existing theoretical frameworks that explain particular aspects of users' data sharing decisions. We begin outlining their limitations in terms of depth or breadth of scope, which we will re-examine in the discussion in §7.1.

One of the most prominent frameworks focused on contextual factors is the Theory of Privacy as Contextual Integrity (CI) [83–85]. CI characterizes context in terms of roles, goals, and behavior-guiding norms that have evolved in societies over time, which prescribe information-sharing practices in these specific social scenarios. For example, in a medical context, there is a specific set of norms that define and limit what information about patients' health is appropriate for providers to share with others and when, relative to healthcare goals [43, 86]. CI predicts that privacy violations occur when an information exchange does not conform to the established contextually-specific norms about information flows [e.g., 10, 11, 19, 65, 83, 84].

CI outlines five contextual parameters describing information transfers: data subject, sender, recipient, data attribute (i.e. information type, topic, or content of the data), and transmission principles (how the data is shared, or under what conditions). For example, in Vitak and Zimmer's examination of varying public reactions to different types of Covid-19 contact tracing apps, they compare the differences in reactions depending on the situation: which *recipients* (government agencies vs. potential contacts) receive which *data attributes* (location vs. time of exposure) of *data subjects* (app users) from the *senders* (the apps) according to which *transmission principles* (via centralized database vs. via on-device storage; allowing secondary use for tracking population movements vs. limiting secondary uses).

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*, for example, whether and how to share a specific piece of information. Moreover, while the vagueness of the concept of *transmission principles* allows for flexibility, it makes it difficult for the theory to provide a systematic accounting of their role in sharing scenarios.

Communication Privacy Management Theory (CPM, or Communication Boundary Management Theory) [64, 90, 91] also includes in its model contextual factors that affect how people form information disclosure rules and draw boundaries between public and private information. 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. However, CPM does not further specify what in particular might define a given context.

Similarly, Altman's Boundary Regulation Theory (BRT) [6, 7] holds that privacy is not static and does not have universal rules, but is a dynamic, situationally specific, and selective process of control of access to the self. A person's desired level of privacy is continuously changing in response to situational factors and circumstances, such as cultural practices and social relationships and processes, along with more general individual tendencies [7, 88, 101]. BRT considers these situational factors and circumstances as context. BRT focuses on balancing intrusion avoidance and loneliness avoidance, but does not consider a variety of other goals the decision maker may have.

Protection Motivation Theory [98] and Technology Threat Avoidance Theory [57] posit that users' decisions to avoid privacy-related threats are determined by their perceptions of how likely they are to experience such threats, their level of severity, and whether they perceive themselves as capable of protecting themselves. However, these theories focus on *avoiding involvement* in information exchange, and do not explain *decisions to share* information. This provides only a narrow window on context, focusing on risk perception and protection.

Finally, the Privacy Calculus approach [35, 36] 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 also considers context narrowly, focusing on the cost-benefit analysis, and does not consider, for example, the impact of emotional reasoning, attitudes, and the effects of incomplete understanding.

The works cited in §2.1 have demonstrated empirically that information sharing preferences are heavily dependent on context. However, those works are not systematic in describing context, and explore the effects of different factors in isolation. Theoretical attempts to define such contexts and explain the relationship between contextual factors and information-sharing decisions are also fragmented, limited in scope, and too general to capture the practical complexity of the decision-making process. These limitations make it hard to explain or predict information-sharing decisions. As privacy regulations and the design of privacy-protecting technologies depend on understanding users' information-sharing behaviors, expectations, and preferences in context, there is an urgent need to model more comprehensively what that context encompasses. Our work offers both practical and theoretical contributions in this regard. We expand the notion of context compared to prior work and provide a systematized analytical model of contextual factors that affect information-sharing decision-making, along with empirical evidence for those factors.

3 METHODOLOGY

With IRB approval, we conducted 1–1.5 hour semi-structured interviews with 46 English-speaking older adults without self-reported serious cognitive impairments (such as dementia or Alzheimer's) in May–June 2018. We recruited participants via nursing homes, senior residences, senior centers, and cultural organizations for retired people in the San Francisco Bay Area, offering $20 compensation. We discussed: (1) what information they do and do not expect various devices to collect about them, (2) what information they feel comfortable having collected or shared, (3) with whom they would be comfortable sharing this information, and (4) how this information can be used or misused.

While our sample may not be fully representative, it is diverse in terms of level of independence, health, and living arrangements (see §4). More information about recruitment strategies and data collection can be found in Frik et al. 2019 [39], in which we present findings from a separate set of questions on privacy and security threat models, concerns, and mitigations.[1] (In contrast, this paper focuses on opinions about information flows and information-sharing decision making.)

Three researchers independently developed initial codebooks using open coding of transcripts. The initial codebooks were merged, and disagreements were jointly resolved. Four researchers (the

[1] Interview guide: https://tinyurl.com/interview-guide-seniors. Entry and exit surveys: https://tinyurl.com/survey-seniors.

three who developed the codebook plus another) used this codebook to code (or recode) all of the transcripts, with two researchers per transcript.

For the scope of this paper, we focused on a subset of codes related to information-sharing decision making (such as "okay to share," "not okay 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. 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, we do not attempt to reach quantified conclusions. (We will explore this in future survey research; see §7.1.3.) Instead, in line with widely recognized norms of qualitative research [e.g. 12, 18, 113], we demonstrate the dependability of the findings via a detailed description of the analytical procedures and by supporting the findings with abundant quotes.

4 PARTICIPANT CHARACTERISTICS

Our 46 participants were 65–95 years old (mean=76), 65% female, and mainly white (76%). The majority have an advanced (44%) or Bachelor's (33%) degree. Most live alone (63%), live 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).

Amongst our participants, most used mobile phones or smartphones daily (52%) or at least sometimes (22%). Similarly, most used computers or laptops daily (61%) or sometimes (22%). Daily tablet usage was less common (22%), similar to only-sometimes usage (24%). The percentage of our participants that use all three, 39%, is similar to the figure for the general adult US population, 36% [9]. Just 11% of the participants do not use any of those devices.

Limitations. Our sample is diverse in terms of income, level of independence, health, and living arrangements. However, our sample overrepresents people with advanced education and white (non-Latinx) ethinicity, and the study was conducted in an urban/suburban high-tech center, with relatively many services for older adults, including computer classes. These factors may limit the generalizability of the sample.

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. When we asked participants what information they would feel comfortable or uncomfortable sharing, 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 (before we had asked about those aspects). 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., 3, 10, 14, 50, 56, 65, 80, 83, 84, 87].

5.2 Use of Paradigm Examples

While some participants described detailed scenarios and conditions for information sharing, others used paradigm examples as shortcuts in expressing their sharing preferences—i.e., the participants seemed to view those examples as obvious and not requiring explanation: "*I just wouldn't want anybody to get into my medical records. I mean, that's personal information that is mine. I don't want everybody to know it.*" (P14) In such examples, one core element of information flow (usually information topic, or recipient) was often used to represent the sharing scenario, while other elements of the scenario (e.g., purposes of information sharing or use, benefits, and risks) were implied rather than explicitly enumerated (see §5.2.2). Using thematic analysis, we identified several such example scenarios common in our data.

5.2.1 Views on sensitive data types. Participants often used financial data and medical records as paradigm examples of sensitive data types. In the rare examples when participants said that they would be willing to share such data, they often highlighted that it was only in the context of very trusted relationships: "*[My brother] shares my checking account with me. [...] So if something happened and I was unconscious, he could go in and make sure my bills were paid and stuff.*" (P24)

Interestingly, while phone number and physical address were often considered sensitive contact details, few participants mentioned email addresses as sensitive or valuable. This may be related to the fact that older adults use email less frequently than younger people [100], and typically to communicate with a restricted circle of known contacts[99]. Thus, threat models involving abuse of phone and address information may be more available to older adults, who often reported concerns or experiences with telemarketing, robocalls, and risks of physical harm and burglary. Almost the only risk participants mentioned related to sharing email addresses was email spamming, which may be perceived as less annoying or dangerous compared to robocalls. Only a few respondents were concerned about email scams or about unauthorised access to their email, and no one mentioned risks associated with using email being used to reset credentials for other accounts. Low awareness about these threat models may explain why email address was rarely perceived as a sensitive data type.

5.2.2 Recipients and purposes. When talking about recipients, respondents often evoked a combination of *who* receives the data and *what* they are going to do with it (cf. [5, 11, 84]). 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.).

Our respondents were commonly willing to share (or at least not opposed to sharing) 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 (benefiting the data subject or society as a whole). Frequent paradigm examples of benevolent recipients included medical staff and close connections (family, friends). Among personal benefits, those most frequently mentioned were related to safety, emergency assistance, and healthcare, followed by more general assistance, such as providing recommendations, enabling home control, or assisting in navigation.

On the other hand, frequent paradigm examples of dispreferred recipients were "hackers" or "attackers," descriptions that imply obvious malicious goals. In addition to such obviously malicious actors, participants often expressed concerns about strangers and unknown recipients, and about companies obtaining data without explicit consent and using it to the data subject's detriment (e.g., for unsolicited marketing or targeted advertising). However, sometimes respondents were not opposed to sharing data with system developers and device manufacturers, but only if the purpose would be limited to provision of a primary functionality.

5.3 Disentangling Contextual Factors in Paradigm Scenarios

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., 92], or to quantify the value of privacy [e.g., 3]. In our data, while paradigm examples were common shortcuts that participants used to express their willingness or unwillingness to share information, further probing revealed more complexity.

In addition, judgments on those examples were not unanimous among our participants. Participants might be unwilling to share certain information that might seem innocuous to most people, even with their family or friends, where feelings are at stake: "*The people close to you are the ones that are most likely to be hurt by information that I consider to be inappropriate. [...] I am more concerned about a friend of mine hearing that I have been friends with [that friend's ex-wife, post-divorce]. [...] His feelings would have been hurt.*" (P121) Some participants thought medical information should be shared more freely, for example if they thought restrictions impeded care: "*I wish the doctors would interface with the preferred provider plan that I have, but they don't. So, I had the responsibility to interpret different things that they are not aware of. [...] It is so compartmentalized, that is what is really frustrating about... It is a benefit and it is a curse.*" (P46) A few did not even object to publicly sharing 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) 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 highly heterogeneous opinions, often with opposite valences, and often depending 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.

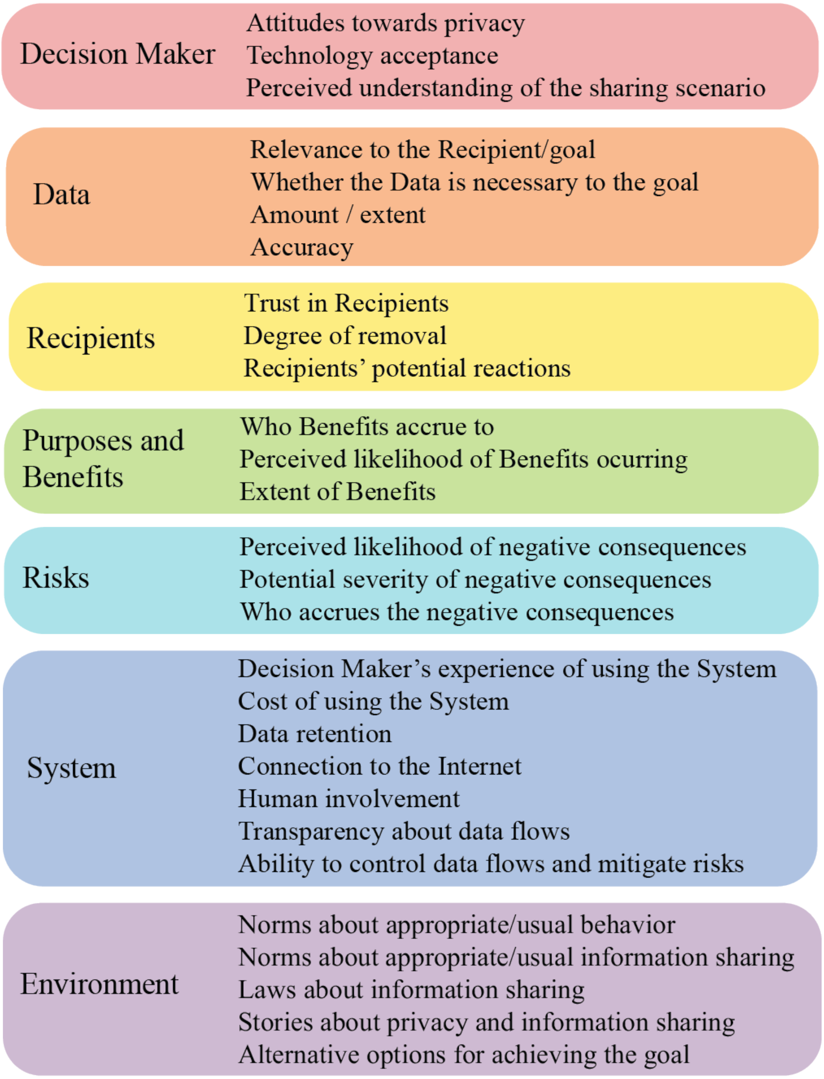
The model is organized as follows:

(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 evaluation of the recipient's (good or bad) intentions*, and *evaluation of the recipient's intentions* (sub-factor) in turn contributes to *trust in the recipient* (factor).

Figure 1 provides an overview of the factors, organized into dimensions, and Appendix A provides a complete listing of dimensions, factors, sub-factors, etc.



Decision Maker
Attitudes towards privacy
Technology acceptance
Perceived understanding of the sharing scenario

Data
Relevance to the Recipient/goal
Whether the Data is necessary to the goal
Amount / extent
Accuracy

Recipients
Trust in Recipients
Degree of removal
Recipients' potential reactions

Purposes and Benefits
Who Benefits accrue to
Perceived likelihood of Benefits ocurring
Extent of Benefits

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

System
Decision Maker's experience of using the System
Cost of using the System
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 about information sharing
Stories about privacy and information sharing
Alternative options for achieving the goal

Fig. 1. The proposed qualitative model of contextual information-sharing decision-making: Dimensions and top-level factors.

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.
- **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 [28, 39, 104, 112], and is the foundation of the Privacy Calculus [36]. 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.

For ease of use, the flow of the model (see Figure 1) 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 Purposes that may incur some Benefits 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 in question, are in italics and give a reference to the subsection where they are described.*

Caveats. The model has a few caveats:

- We have grouped the identified factors into dimensions in order to be able to represent them systematically. However, these groupings do not have consequences for the interpretation or use of the factors in the model. As we noted in §2.2, our decision to organize factors along the chosen dimensions is in part driven by what could be most useful for designing and evaluating systems.

- Identified lists of factors and contributing sub-factors represent the themes we identified in our data, but are not intended to be exhaustive.
- 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 there being any identified sub-factors contributing 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 use 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 enter into their decision. For example, if a decision maker is not aware of a particular risk, we assume that that risk does not affect their decision about sharing information.
- Participants sometimes used examples from offline interpersonal communications, for example, whom they would trust enough to tell about a medical problem in person, as reference points while they deliberated over their answers to our questions about online sharing. While offline behaviors do not necessarily translate directly to online behaviors [cf. 77], we did include some offline examples given by participants in developing the model, where participants were using those examples to explain their reasoning about online information-sharing decisions.

6.1 Decision Maker Dimension

Factors in the **Decision Maker** dimension:

- Attitudes towards privacy
- Technology acceptance
- Perceived understanding of the sharing scenario

The decision maker in our model is a person who is making a 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, rather than, say, empirical data about effects of attitude on privacy behaviors.

6.1.1 Attitudes towards privacy.

Decision Maker > Attitudes towards privacy

Sub-factors contributing to this factor:

- Desire for agency and control
- Circumstances that make the decision maker feel especially vulnerable to certain risks
- Personal experiences with privacy or security violations
- *Environment > Norms about appropriate or usual information sharing (§6.7.2)*

Attitudes toward privacy comprise individual opinions and beliefs about one's personal information, and general willingness to share it. Participants recognize that privacy attitudes may differ among individuals: "*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) In addition to general attitudes, some participants cited attitudes specific to particular data types or topics: "*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.*" (P22)

Participants sometimes expressed their privacy attitudes in terms of the degree of ***desire for agency and control*** they want to have over their personal information: A person who is uncomfortable losing agency may be less willing to allow data out of their control: "*The one thing you lose as you get older is control, so you hold onto it. Even when you shouldn't at times.*" (P24) Alternatively, they may be more willing to put in extra effort to monitor and control how and with whom their data is shared: "[Interviewer: Can you imagine how they could misuse this information? [...]] *Well, they are tracking everything I buy. [So] I do most of my Internet research [...] on Mozilla Foxfire [sic], and then I have it set so that when I close Mozilla Foxfire, all the cookies are deleted. [...]* [I: Did you find [the settings] yourself, did you read about it? [...]] *I asked and researched.*" (P108) While some participants described the *desire for agency and control* as a general individual trait, others framed it as a fundamental right of ownership over one's personal data: "*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)

Some participants expressed a specific concern about whether they are the one who actively initiates the data collection or sharing themselves: "*I wouldn't want [my psychologist] 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 participants, 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. [...] Not everybody can fix everything.* " (P107)

Circumstances that may make a decision maker feel especially vulnerable to certain risks include particular historical background; socioeconomic, financial, or living situation; health conditions; political or religious beliefs; ethnicity; and sexual orientation (see more extensive discussion in Frik et al. [39]). These circumstances may increase perceived sensitivity of personal data, and may cause decision makers to be more hesitant about sharing: "*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 end of the spectrum, people who believe that no particular circumstances make them especially vulnerable to certain risks may feel less concerned about their privacy. People may view this as meaning they have "nothing to hide," when 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)

Personal experiences with privacy or security violations can also affect a decision maker's privacy attitudes. For example, several participants commented that after falling victim to scams, they became more cautious about sharing. However, past experiences with violations do not increase concern for everyone, and in some cases may even desensitize the decision maker: "*I wouldn't be uncomfortable with any of those [types of data]—the kinds of appliances I use and my communication. I went through a period where my phone was tapped for three years; it doesn't bother me.*" (P35)

6.1.2 Technology acceptance.

Decision Maker > Technology acceptance

Sub-factors contributing to this factor:

- Technology self-efficacy
  - *Decision Maker > Perceived understanding of the sharing scenario (§6.1.3)*
- Circumstances that increase the need to share certain information

A decision maker's degree of **technology acceptance** can also be described as their general attitude towards using technology, including to share information. For example, some people like the convenience and speed of electronic information sharing: "*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)

Technology self-efficacy is the decision maker's belief that they can successfully use 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.*" (P44) Participant 46 specifically mentioned 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)

A decision maker's sense of *technology self-efficacy* may depend in part on how well they feel they've *understood the sharing scenario* in particular situations they've encountered (§6.1.3). For example, participant P20 does not understand how data flows between different services, and so feels discouraged from taking action to protect herself: "*I'm not that knowledgeable about all the ways that accounts can be vulnerable. Bank accounts, I mean, or even credit card accounts.* [I: [...] What would you do to have your account more safe from the concerns...?] *Well, I was thinking of cancelling my Facebook account, but then I read that even if you're not a member, that they can get all kinds of information, so I don't know if I want to bother with that.* " (P20) The relationship is reciprocal; at the same time, a decision maker's perception that they will be able to *understand a specific sharing scenario* depends in part on their general feeling of *technology self-efficacy* (see §6.1.3).

Certain ***circumstances may increase the need for collection and sharing*** of certain personal information, and therefore may affect acceptance of the technology that collects it. For example, the decision maker's state of health may affect their acceptance of devices that collect and share vital signs: "*Given my situation, my health, [a wearable fitness tracker] is something that isn't high on my list. [...] I know people who wear various kinds of monitors [because of] a specific reason. They are subject to high blood pressure, they are subject to pulse fluctuating wildly, and so forth.* " (P121)

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. [...] There is a number of people around here that have a pendant [alert button]. [...] As long as there is two of us, we probably won't get them.*" (P123)

6.1.3 Perceived understanding of the sharing scenario.

Decision Maker > Perceived understanding of the sharing scenario

Sub-factors contributing to this factor:

- Past experiences with similar or related data sharing scenarios
- Knowledge of the specific data flows and mechanisms involved
- *Decision Maker > Technology acceptance > Technology self-efficacy (§6.1.2)*
- *Environment > Stories about privacy and information sharing (§6.7.4)*

A decision maker's assessment of whether their privacy expectations are likely to be correct, i.e. the **perception of their own ability to understand the data sharing scenario** in question and to predict the potential consequences (including benefits and risks) may affect their decision about whether to share some data. For example, P123 is hesitant about cloud services: "*I don't use a wireless backup, a cloud backup [for financial data]. [...] 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) Such knowledge may rely on analogies with more familiar technologies (cf. [76, 116]), for example, when the decision maker forms expectations about the data practices of a smart speaker (e.g. Alexa) based on prior knowledge about mobile voice assistants (e.g. Siri).

This self-assessment of understanding may rely in part on whether the decision maker has had ***past experiences with similar or related data sharing scenarios*** (including their benefits and risks): "*The two times that [identity theft] has happened to us, routine controls would stop those things from happening. [...] 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 of the specific data flows and mechanisms involved*** in the situation under question: "*I used to do consumer product stuff. [...] Before, [data] 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. [...] I think we might have been more aware in the past of that than we are now.*" (P71) Note that this subfactor encompasses any knowledge that the decision maker thinks they have, whether or not we view their assumptions as correct: "*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. [...] I don't know whether it's the broadcasting station or whether other people can do it, but I just know that it's possible that they could see what you are doing.*" (P25)

When making a sharing decision based on some factor (other than Decision Maker factors), a decision maker may be believe themselves to be relying on specific, concrete knowledge about what is happening or what is supposed to happen with their data; they may be relying on assumptions and expectations about what they believe to usually be the case; or they may feel like they don't have enough information at all.

6.2 Data Dimension

Factors in the **Data** dimension:

- Relevance to the recipient/goal
- Whether the data is necessary to the goal
- Amount/extent
- Accuracy

The Data dimension describes the particular characteristics pertinent to a specific piece of data (e.g. the decision maker walked 3.3 miles on March 3) or to a category of data (e.g. daily exercise levels) that may affect participants' decisions to share that data.

As we noted in §5, some theoretical models and empirical studies focus on determining the sensitivity of *categories* of data—"data types" or topics (such as medical or contact information)—rather than on *characteristics* of that data. Yet research consistently finds privacy preferences and behaviors to be idiosyncratic and context-dependent [e.g. 10, 14, 65, 80, 83, 84].

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). However, in the same vein as the research mentioned above, we believe these paradigm examples and gestalt judgments of invoked scenarios are in fact a product of the interplay of several different factors. In the interviews, we probed 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 okay.*" (P13)

In our analysis, we therefore aimed to dissect participants' explanations of their decisions, to identify 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 other characteristics belong to other dimensions of 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 decisions in terms of the data's **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: "*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.*" (P47) Some participants prefer not to share if they do not believe it will 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 (own) 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 benefiting themselves. But sometimes participants also talked in terms of data's relevance to achieving the goals of 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—for them to know that someone like me went through those things all those years ago that might help them currently.*" (P35)

6.2.2 Whether the data is necessary to the goal.

Data > Whether the data is necessary to the goal

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 the data is *necessary* to achieving the decision maker's goals** in sharing it. 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) Optimal function was also a consideration: "*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 systems sometimes request data they do not need—or arbitrarily require it as a condition of providing a service—when their purpose could be achieved without the requested data, with less data, or with a different type of data: "*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 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 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 (§6.6.3)*
- Granularity/specificity
- Data format and type of sensor

The **amount or extent** of the data that could be collected can affect sharing decisions: "[I: I'm curious about why you feel that 'OK Google,' like on your phone, is okay, and Alexa is not?] *Because it's in your home. Well, so is your phone, I guess. But I think they can capture more information.*" (P104)

Concerns about amount 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 §6.6.3). 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 advance 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 ***data format and 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 examples 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 *whether the data is necessary to the goal* (§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, ongoing data collection and accumulation may produce more *accurate* inferences and better achieve the purpose of collection (§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) also may (or may not) offset the negative aspects of ongoing monitoring, such as contributing to the *perceived likelihood of negative consequences* (§6.5.1): "*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.*" (P103)

6.2.4 Accuracy.

Data > Accuracy

In sharing decisions, some participants consider the likely degree of **accuracy** of the data. For instance, some are concerned that sharing access to data may result in inaccuracies introduced by the new recipients: "*[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)

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. in other dimensions).

For example, many of the explanations of what makes a data type or piece of data sensitive were related to the *likelihood* and *severity of negative consequences* (§6.5.1, §6.5.2) should it become more widely known. In particular, sensitivity related to risks could arise 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 about 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) for that particular type of data. On the other hand, participants also drew connections between their own general *attitudes towards privacy* (§6.1.1) and their views on the sensitivity of particular data types or topics. Finally, participants might refer to the fact that some piece of data, or the information it implicates, is already widely known—in other words, they define 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 only a few examples where participants considered situations where they were the decision maker and someone else 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 acknowledged that the data subject might have different preferences than their own, the participant 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, '[...] I'm having my daughter become power of attorney,' or something like that. That's nothing anybody needs to know. So at least [using 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, 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-sharing decisions could be different for information about other data subjects [cf. 75]. 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.

The *data subject* role is also used in previous literature to cover the effects of identity characteristics. Identity characteristics, including personal or sociocultural aspects, and identity-based vulnerabilities, are analyzed in this model as factors related either to the social context that defines appropriate behavior and information-sharing practices relevant to those identities (see §6.7.1), or to the decision maker (see especially *Circumstances that may make a decision maker feel especially vulnerable to certain risks* in §6.1.1), again because the decision maker and data subject were highly interconnected in our data. (Further research can isolate the effects of sociocultural identities of data subjects who are not the decision makers.) Another important use of the construct of data subjects, especially in literature on Contextual Integrity [e.g. 84, 86], is in mapping entities onto their context-specific roles or relational identities, such as the data subject being the Patient in a healthcare scenario. In our model, these considerations are analyzed in terms of the relationship between the decision maker and the recipient and the alignment between their goals (see, e.g., §6.3.1) and the relevance of the data to enabling the recipient to achieve the goal of sharing (see §6.2.1).

6.3 Recipients Dimension

Factors in the **Recipients** dimension:

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

The Recipients dimension relates to 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. friend, physician, salesperson, hacker). However, such categories do not carry universal implications; rather, they often represent an interplay of different factors affecting decision-making. 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 recipients.

Recipients > Trust in recipients

Sub-factors contributing to this factor:

- Evaluation of recipients' legitimacy and (general) intentions
  - Past experiences within the relationship
  - Recipients' reputation
    - *Environment > Stories about privacy and information sharing (§6.7.4)*
  - Assessment based on appearances
- Evaluation of recipients' judgment and competence/ability
- *System > Ability to control data flows and mitigate or protect against risks (§6.6.7)*

Trust in the recipients reflects a belief that the recipient(s) will not use 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 (at least with a narrow set of relevant information, such as medical records): "*I would have no reason for [my family doctor] 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 [with my doctor and my son] because I trust them.*" (P20) They tend to have the least trust in strangers, marketers, or obviously malicious recipients like hackers: "*We already know all of the hackers and misusers are out there, the deviant-type people. And to include all of the people that are sabotaging the computer and hacking into your financial stuff, hacking into your personal stuff.*" (P9)

However, as we mentioned earlier, even with a usually-trusted type of recipient like family, decisions may differ based on more specific characteristics: "[I: Would you be comfortable sharing [medical information] to family or friends?] *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 [...] and they want to say 'This person, [...] she's not competent to handle her own life.'* " (P47)

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)

Trust may be based on a decision maker's ***evaluation of a recipient's legitimacy and whether they have (generally) good intentions***. Such beliefs may rely on *past experiences within the relationship*, for example with their friends or businesses: "*I gave her my credit card number and everything. [...] This friendship is 40 years, and you know, there was no question about that.*" (P34) "*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) *The recipients' reputations* can also be a factor; for example, participant P121 said he would be comfortable sharing if "*a reputable organization, which is well-managed, is collecting information*" (P121). When users are not familiar with the system or service, they may have to make an *assessment based on appearances*: "*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 the decision maker, a negative ***evaluation of the recipients' judgment, i.e. wisdom, and their actual competence and ability*** to do it, may undermine a decision maker's trust: "*I just hope [the manufacturer] can keep [my usage data] in the same place and it will not be hacked.* [I: Would you trust or not trust companies in that?] *Not. [...] Because the hacker, they are very advanced, you know, they can do anything. Even the IRS or Social Security, [...] They have all the money, they get [...] the most advanced expert to do those prevention. But if they fail to do it... And you just do small company, is almost impossible.*" (P103)

When a decision maker is thinking about a service provider or System as itself being the Recipient, their *trust in the recipient* is also affected by whether that system provides them with the *ability to protect against or mitigate potential risks* (§6.6.7): "*I use [Duck Duck Go] because I don't get as many ads. If I use Google then I look at something online, then I get ads forever. So they obviously keep track of it even if I... I get rid of my cookies all of the time and I am not... I just... It's so weird.*" (P24)

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. The more intermediaries there are between the decision maker and the recipient, the less control the decision maker perceives themself to have over the shared information: "*What happens when you go onto 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 as though the decision maker were considering what they'd share with that human recipient in person—even if the question was about using technology (i.e. an intermediary) to share, and thus the person in question would actually be a secondary recipient.

6.3.3 Recipients' potential reactions.

Recipients > Recipients' potential reactions

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 **recipients' potential reaction** to that information.

For example, some participants mentioned their ***perceptions about the recipients' desire to receive the information***, saying that they did not share data when they expected recipients not to be interested in it: "*I think even my brother and sister, I don't think, that interested in all this [medical] information about me. Only if I need help, I just call them and tell them what I would like them to help me to.*" (P102)

Participants also were reluctant to share information when they expected a negative ***affective reaction*** from the recipients, such as disapproval, annoyance, or worry: "*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 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.*" (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: "[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) In particular, some participants commented that they wouldn't mind sharing information that many people already know: "[I: 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 out there already.*" (P22)

⇆ Connections and Trade-Offs ⇆

Although participants mostly mentioned *likelihood that the recipient already knows or could easily guess* as an explanation in itself for why they might share a particular piece of information, some connected it to a generally unconcerned *privacy attitude* (§6.1.1)—i.e. that they generally don't worry because they assume *everybody* already knows or easily could know anything there is to know about them: "*I am not sure if I trust [the smart speaker] or not. But [...] I don't worry about it that much anymore. Especially at my age.* [I: Why especially at your age?] *Oh, they are not going to find anything about me that nobody else doesn't know already, so. Plus, I tell everybody everything I do, so there is not secret.*" (P33)

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

The Purposes and Benefits dimension describes the recipient's purposes in collecting the data, i.e. what the recipient intends to use it for and what benefit that use is intended to achieve.[2] Many of our participants expressed the importance of knowing the purpose of data collection and use, even with likely-benevolent recipients (see also §6.6.6): "*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.

Domains of benefits. We can categorise benefits discussed by our participants into three broad domains. Material benefits include financial gain, for example by lowering medical or housing costs, or qualifying for subsidies. Benefits related to physical health and safety include emergency response, medical diagnostics, and incentive to exercise or take other steps to improve health. Intangible benefits include emotional support and feeling of connection, time savings and convenience, and recommendations of interesting or useful content. Due in part to the focus of our interviews, health and safety benefits came up frequently and constitute the majority of the examples in this subsection, but material and intangible benefits were discussed in similar ways.

6.4.1 *Who benefits accrue to.*

Purposes and Benefits > Who benefits accrue to

Participants were interested in **who benefits will accrue to**, in particular whether the recipient's purposes in collecting the data could potentially benefit the decision maker, 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 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 [smart watch] I see not really, it didn't seem to influence it that much.*" (P26)

Benefits may also accrue to the decision maker's close connections, such as family and friends: "*Health-wise, with all the DNA this, and so forth and so on, if I had any kind of running disease, something came up that I hadn't been tested for, [my family] hadn't been tested for, they would have the knowledge.*" (P21) When those friends or family are the Recipients, sharing personal information may (the decision maker assumes) serve to educate or motivate them: "*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.*" (P6)

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: The social component of helping others may sometimes even play a bigger role in

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

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)

Participants typically responded negatively to 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). 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 in exchange, sometimes. It's 'Facebook is free!' So you give up all this information, because it goes to advertisers.*" (P71)

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

⇆ Connections and Trade-Offs ⇆

Going beyond references to generally good intentions, some participants frame discussions of *trust* (§6.3.1) specifically in terms of their degree of confidence in the alignment between their purpose for sharing the data and the recipient's primary purpose in collecting and using that data. The relevant *purposes and benefits* in its turn may be defined broadly or specifically. In some situations, alignment with recipients' general (broad) good intentions is enough, insofar as they benefit the decision maker. In others, alignment of the specific purposes is important. In the latter type of case, the recipients' purpose may be not explicitly malicious (for example, it may be aimed generally at improving the decision maker's health), but because it is misaligned with the decision maker's own goals, it may still negatively affect a 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 (§6.3.1) is sometimes played off against the *relevance of the data* (§6.2.1) at the same time as the *purposes and benefits* of data 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)

6.4.2 Perceived likelihood of benefits occurring.

Purposes and Benefits > Perceived likelihood of benefits occurring

Sub-factors contributing to this factor:

- *Decision Maker > Technology acceptance (§6.1.2)*
- *Data > Relevance to the recipient/goal (§6.2.1)*
- *Recipients > Trust in recipients (§6.3.1)*

The **perceived likelihood of any benefits occurring** that would accrue to the decision maker or ratified others affects sharing decisions. For example, participant P31 would be willing to share data about her stove usage with a company that notified people when they forget to turn off the gas: "*Because I had experience a couple times, maybe that's important to me.*" (P31) Similarly, participant P102 would be comfortable sharing presence data (i.e. where in the house she is): "*Because like kitchen and bathroom, those are the places that is more dangerous that my fall.*" (P102)

Benefits might be less compelling when they are only vague possibilities: "*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 benefits
- Urgency/time sensitivity of receiving the benefits

The **extent of benefits** describes the perception of how helpful overall the benefits could be (to the decision maker or ratified others), for example in terms of their *importance or added value for the party who accrues the benefits*, and/or the *urgency or time sensitivity of receiving the benefits.*

Importance or added value is often a driving factor for adopting technology in general (see §6.1.2) and for accepting information collection and sharing, specifically: "*[The wrist-wearable pedometer is] obviously collecting information that somebody else is going to know about you. [...] 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 is even sometimes cited 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)

⇆ Connections and Trade-Offs ⇆

Specific to the *privacy attitudes* of older adults, participants living in a senior living facility often mentioned an attitude of resignation about privacy (§6.1.1). They may be willing to sacrifice some privacy if they believe the *extent of the benefit* they will get is sufficiently valuable. For example, privacy might be exchanged for institutional care or better health outcomes: "*You cede a lot of your personal privacy rights when you move into a place like this [nursing home], 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) Or, on the other hand, privacy might be exchanged for continued independence: "*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) This trade-off between desire to avoid privacy risks and *extent of benefit*, particularly the *added value* a decision maker gets from sharing data, could also be relevant to life's smaller choices: "*When I go in the city, instead of getting on the bus, it is easier, call Uber. [...] But I have discontinued that. But 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.*" (P46)

Technology acceptance (§6.1.2) also interacts with the *purposes and benefits* of sharing, and especially with the *extent of the benefits* or *importance or added value* to the decision maker: "[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* (§6.1.2)—and those factors can at the same time be played off against *privacy attitudes* (§6.1.1) and/or against the *perceived likelihood* and *perceived severity of potential negative consequences* if they share (§6.5.1,

§6.5.2): "*When I hear the latest news stories about Facebook this or that, I just go, 'Well, I don't have to be scared,' because I'm [...] 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? 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. [...] And then, be just more anonymous, more protected, more private, which is just sort of the person I am.*" (P47)

Finally, sometimes participants brought up *accuracy of the data* (§6.2.4) in terms of whether data would be useful or *relevant to achieving the purpose of sharing* (see §6.2.1) and thus how it affects the *likelihood* and *potential extent of the intended benefit* (§6.4.2, §6.4.3): "*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. [... But] it is very, very hard to get dependable performance in old people.*" (P121)

6.5 Risks Dimension

Factors in the **Risks** dimension:

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

The Risks dimension describes the potential threats associated with data sharing. Typically, recognised risks negatively affect decisions to share data.

Domains of risks. Similarly to Benefits, we can categorize the Risks mentioned by our participants into three broad domains. Material risks can include financial losses, identity theft), property damage (for example, a robbery facilitated by shared data), exposure to liability, or loss of benefits to which the data subject was otherwise entitled. Risks to physical health and safety could include medical errors, attack by a stalker, or even death due to a hacked medical implant. Intangible risks often carry emotional or social consequences for the decision maker or others (see also §6.3.3). For example, online harassment, government oppression, or unsolicited targeted advertising can lead to emotional distress, waste of time, or reputation damage. We discuss in more detail examples of risks in various domains, participants' privacy and security concerns, and mitigation strategies that arose in our interviews in a separate paper [39].

6.5.1 *Perceived likelihood of negative consequences.*

Risks > Perceived likelihood of negative consequences occurring

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
  - *Recipients > Trust in recipients (§6.3.1)*
  - *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 (§6.6.4)*

  - *Environment > Stories about privacy and information sharing (§6.7.4)*
- Potential inferences from the data
- Reusability of the data across contexts
- *Data > Amount/extent (§6.2.3)*
- *System > Data retention (§6.6.3)*
- *System > Ability to control data flows and protect against or mitigate risks (§6.6.7)*

A decision maker may consider the **likelihood of any potential negative consequences occurring** due to information sharing. Such potential negative consequences may be related or unrelated to the recipient's purpose in collecting and using the decision maker's data.

In the former case, the decision maker makes an ***assessment of whether the recipient's primary or secondary purposes carry risks*** for anyone (see §6.5.3). This assessment in part depends on the *expected material value of the data to the recipient*. For instance, when decision makers cannot imagine how the recipient could extract value, they tend to view the probability of misuse as being lower: "*I think that I am not a focus of whatever these companies are looking for. They probably look at my data—if they look at it–and say, 'Oh, don't bother with her. She's too old to participate,' or maybe 'doesn't have enough money,' or I don't know what they think.*" (P110)

The assessment of likelihood of risks 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: "[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 [that]?] *I just don't trust, there's so many hackers nowadays, that get into your computer. [...] They might hold of my identity and credit card, and take things out of my bank account.* " (P13) The likelihood of risks may be viewed as being higher in certain situations, 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)

Some participants noted that the likelihood of risks (especially of more severe risks; see §6.5.2) may depend not only on the data that is shared directly, but also on the ***potential inferences that could be made from this data***. For example, when asked what information he 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.* [Later, asked how the information that he's at a bathhouse could be misused:] *Well, it could be interpreted. Surmised.*" (P9) In particular, aggregated information can be seen as increasing the potential for meaningful inferences that can be misused (see also §6.2.3): "*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)

Participants also mentioned the potential for risks associated with the ***reusability of certain data across contexts***, e.g. for authentication or identity theft: "*I don't like [Facebook] knowing my age, I don't like them knowing my birthday, where I went to college, the whole thing. [...] I don't like to put my data out there because [...] you can be hacked, and people can impersonate you.*" (P46)

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. For example, participant P5 compares searching for information online (which she does) vs. banking online (which she doesn't do): "*I was looking up pictures of flowers [...] so I now keep getting ads about flowers. [...] Whatever you look up, you get an ad about that thing right on your computer.* [I: And how it sounds like you don't love it, but...] *Well, I know that there are a lot of people are watching what you do on the computer, so I don't do anything. Well, I don't have any secrets anyway, but I mean, I don't want a bank account on my computer. I think that that could be hacked in.* " (P5) Consequences can range from the annoyance of ads to the significantly time-consuming and/or financially damaging: "*I'd be very careful about any banking information. [...] I don't want identity theft. I hear it's a total nightmare. Takes two years, you know, to get it straightened out.*" (P10)

6.5.3 *Who accrues the consequences of risks.*

Risks > Who accrues the consequences of risks

Those **who accrue the consequences of risks** may include the decision maker, her close connections, society as a whole, and/or the recipient(s). Most of our previous examples depict negative consequences that accrue to the decision maker. However, a few participants mentioned concerns about risks to the decision maker's connections: For example, Participant P35's ambivalence about sharing the information that she had illegal abortions is in part tied to concern for a friend who would, by inference, be an additional data subject: "[I: Anything that you still would not want to share?] *Maybe the fact of having had abortions before they were legal. [...] And the fact that I knew a medical doctor who was a personal friend who helped me out, that maybe the whole world doesn't need to know that.*" (P35)

Others mentioned larger-scale social consequences: "*It could be some political group just like we have right now. [...] If you got enough money, you can hire a group of people to hack into anything now, so that is the only thing that I would think about with smart speakers.* [I: And what they would do, these politic groups?] *Well, like they did now, they tried to screw the elections.*" (P33)

Recipients may also accrue the negative consequences of risks: "*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, and are rather judged as an appropriate consequence if they fail to protect data.

6.6 System Dimension

Factors in the **System** dimension:

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

Systems that decision makers may consider sharing data with or through may include (but are not limited to) hardware devices, software/apps, online services, etc., or combinations of all of those.

The System dimension includes factors related to 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 using the system.

System > Decision maker's experience of using the system

Sub-factors contributing to this factor:

- Intrusiveness of the data collection process
- Effort required to use the system
  - *Decision Maker > Technology acceptance > Technology self-efficacy (§6.1.2)*

A decision about whether to share may be affected by **the decision maker's experience of using the system** that is collecting or sharing the data. For example, a decision maker may evaluate the ***intrusiveness of the data collection process***, especially whether it interrupts or distracts from the decision maker's use of the system:[3] "*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)

If the ***effort required to use the system*** is too high, e.g. due to usability issues or time required for set-up and learning, the decision maker may choose a different channel or become reluctant to share information altogether: "*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.*" (P7)

6.6.2 Cost of using the system.

System > Cost of using the system

Participants sometimes discussed whether it was worth sharing data given the monetary **cost of using the system** to share it: "*Of course a lot of it would depend on cost. Cost is a major factor.*" (P110), including indirect costs like troubleshooting: "*So you have to pay [the technician] eighty-five bucks and he'll press the buttons and clear your screen. [...] So that's another reason why I don't want a home computer.*" (P10)

6.6.3 Data retention.

System > Data retention

Participants who mentioned **data retention** as a decision-making factor typically preferred time-limited or purpose-limited data storage over unspecified or unlimited storage: "*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)

6.6.4 Connection to the Internet.

System > Connection to the Internet

Sub-factors contributing to this factor:

- Transmission channel
- Hosting

[3] Note that by 'intrusiveness' here we mean this sense of interruption or distraction, rather than 'intrusiveness' in the privacy sense.

A few participants mentioned considerations around **whether the system is connected to the Internet** or whether their data would be on the Internet (in their understanding). Sharing data in person or over non–Internet enabled ***transmission channels*** is usually perceived as more secure: "*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. [of] statements, credit cards' bills. [...] I just don't want records out there.*" (P36)

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

⇆ Connections and Trade-Offs ⇆

Participants' concerns about the recipient's *degree of removal* (§6.3.2) could be framed more as being about whether a potential recipient was the *primary* intended recipient than about their place in the transmission chain. In particular, some participants had concerns about *transmission channels* that resulted in additional entities having access to the data along the way to its intended recipient: "*I've used devices, like when you wear a Holter [heart] monitor, and so the information is sent through a telephone to a place where they read the data and then give it to your doctor. So there's a lot of information that can be transmitted by smartphones and other things to third parties, [...] and most of us don't think about the fact that those are privacy disclosure issues. But they are.*" (P71)

6.6.5 Human involvement.

System > Human involvement

The extent of **human involvement** in data collection or analysis runs from fully algorithmic to fully human processing. Human involvement is usually associated with a higher degree of privacy concern, as well as human errors (cf. [32]): "*The person that is– actually that has the keys, knows the password to get into patients' database [...] maybe they've been messed over by their supervisor at [a healthcare provider] and the way they are going to pay [the healthcare provider] back is compromising the patient information.*" (P8) On the other hand, in other situations, some decision makers might prefer humans to be in the loop: "[about care robots] *I prefer communicating with people and being able to ask for what I need.*" (P28)

6.6.6 Transparency about data flows.

System > Transparency about data flows

Participants often mentioned the importance of **transparency about data flows** in their decisions about sharing personal information: "[I: How do you think [a data collection agency] could use this information?] *I have no idea. That's why I wouldn't want them to have it.*" (P69) Transparency can be important even when decision makers are not concerned about the data sharing itself: "*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)

⇆ Connections and Trade-Offs ⇆

In some cases, participants clearly indicated what elements of the system or aspects of the sharing scenario they most want transparency about, such as *recipients* (§6.3): "*I find myself starting to fill things in and then I get partway through, [...] 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) or *purposes* (§6.4): "*I'd have to ask some questions first to see if the device itself was being used other than it was intended.*" (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). We therefore 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.

For example, a Decision Maker's *knowledge of the specific data flows and mechanisms* (and their privacy implications) (§6.1.3) can be supported by improved *transparency about data flows.* Participants mentioned deciding against data sharing due to not having sufficient information: "*Having not purchased these [devices], 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)

Some participants drew connections between *trust in a recipient* service provider (§6.3.1) and their perceptions about the service provider's *transparency* 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. The [device's] capabilities could often result in somebody's abuse of your information.* [Later, defining 'abuse':] *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)

6.6.7 *Ability to control data flows and mitigate or protect against risks.*

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

Sub-factors contributing to this factor:

- Effort required to control/protect/mitigate
  - *Decision maker > Technology acceptance > Technology self-efficacy (§6.1.2)*
- Cost of control/protection/mitigation
- Likely effectiveness of the means of control/protection/mitigation
  - *Recipients > Trust in recipients > Evaluation of recipients' judgment and competence/ability* (§6.3.1)

Participants mentioned concerns about **whether they are 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 may be viewed as a negative consequence 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) or to prevent secondary risks.

In assessing their ability to control, protect against, or mitigate risks, the decision maker may consider whether (to their knowledge) the system provider has taken steps to ensure control: "*Can I specify who I share with? Like Facebook where you can say, 'These are my friends.'*" (P24) and security: "*I trust Apple more than most anyone. [...] If you sign into iCloud, if you have that two-layer security turned on, [...] 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.*" (P123) The decision maker may also consider the existence and availability of other means of control, protection, and mitigation that can be added on from entities outside the system: "*I used to have antivirus but now it's built into Microsoft, so I use Microsoft.*" (P108)[4]

Decision makers sometimes evaluate the time and ***effort required to enact controls, protections, or mitigations***. Effort required can, for example, reflect the convenience and usability of built-in means of data protection, such as password management: "*I use the same password for everything and I have used the same password for years. Even though we have been advised not to do that. [...] 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) 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)

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

The ***likely effectiveness of controls, protections, or mitigations*** was also a question for participants: "*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) A decision maker's *trust* in a recipient service provider or recipient system's *competence and ability* to handle their data appropriately (§6.3.1) can affect their own assessment of the whether protections or controls offered by the system are likely to be effective: "*You purchase this antivirus 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)

⇆ Connections and Trade-Offs ⇆

The model does not attempt to account directly for whether or what a participant knows about any specific control or protection, as it only describes factors the decision maker could be aware of. However, some participants made higher-level comments about how knowledge about protections could affect their decisions, in terms of (general) *Technology self-efficacy* (§6.1.2) and their *Perceived understanding of the (specific) sharing scenario* (§6.1.3): "[I: Would you expect to have some control over this information? If it's your account?] *Well, I would want to, but [...] 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)

Some participants mentioned how their *desire for agency and control* (§6.1.1) affects how concerned they are about having meaningful choices that *allow them to control data flows*: "*If I give my permission for somebody to have [information about me], if I want to share it, then that's fine. They would have to ask me first. I wouldn't want something that would just– They get a list, and then they get hundreds of other people, and then it snowballs.*" (P1)

As with *transparency about data flows* (§6.6.6), we view the *ability to control data flows and mitigate or protect against risks* as acting in combination with other factors elsewhere in the model to specify what a decision maker might want control of.

6.7 Environment Dimension

Factors in the **Environment** dimension:

[4] We include such measures under System because they eventually have an impact on the decision maker's ability to control data flows, and to mitigate 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.

- Norms about appropriate or usual *behavior*
- Norms about appropriate or usual *information sharing*
- Laws and regulations about information sharing
- Stories about privacy and 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. The Environment dimension is distinct from the System dimension in that designers and developers have greater control over factors in the System dimension, while Environment factors should be taken into consideration, but cannot be directly manipulated by 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:

- Laws about behavior

Sociocultural **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 given the content it captures. Our participants often mentioned that they are more open to sharing information about activities that comply with sociocultural *norms about behavior*—whether the norms of a small group or community that they identify with and/or are embedded in, or the larger society—and more reluctant to share information about behaviors that violate such norms: “*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 sharing information explicitly about activities or characteristics that do not comply with *norms about behavior*, a few participants were concerned about how *potential 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

Sociocultural **norms about appropriate or usual 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: “*I don’t think normally people go around sharing how I sleep and all of that. That’s very private.*” (P37) Such norms are often described in terms of the particular context they apply to [cf. 83]: "*I guess if you go to a public place then it is not sensitive, you know.*" (P37)

Some norms can be perceived as specific to a small group, community, culture, identity group, or generation: "*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 [...] or work in tech, probably have a different feeling about it.* " (P71) Alternatively, norms may be defined by the broader society and may (or may not) cross borders: "*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. [...] And that was really hard in the beginning. Because in America, in the States, people shouldn't be knowing that.*" (P24)

Norms about appropriate information sharing inform a decision maker's expectations about various other factors in the sharing situation [83], and may be expressed in terms of what the decision maker *expects* to happen in a given context: "*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 ⇆

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 in analysis. For example, it is unlikely that P32 finds using the bathroom inappropriate in itself, 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)

Some participants highlighted tensions between their individual *privacy attitudes* (§6.1.1) and general *social norms about information sharing*. 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 sensitive to most people: "*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)

6.7.3 Laws about information sharing.

Environment > Laws about information sharing

Participants also referred to **laws and regulations about information sharing**, not necessarily 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)

6.7.4 Stories about privacy and information sharing.

Environment > Stories about privacy and information sharing

Sub-factors contributing to this factor:

- Media stories

- Stories about past experiences of the decision maker's close connections

Stories the decision-maker has heard about privacy and information sharing, for example ***stories in the media*** (e.g. TV, newspapers, online news sites) also affect their decisions about whether to engage in information collection or sharing: "*First of all there's identity theft, which is all over the papers. And that's the big thing. That's the only thing I can think of.*" (P77)

Some participants were skeptical about whether the media is a helpful source of information about privacy and security risks and protections: "*I think [Alexa] 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.*" (P104) The stories the decision-maker has heard about privacy and information-sharing contribute to their *perception of their own ability to understand a sharing scenario* (see §6.1.3); of course, if they are not certain that what they've heard is reliable, that undermines its contribution to their confidence in their own understanding.

Decisions may also be affected by ***stories the decision maker has heard about the past experiences of their close connections***: "*I am the type of person that would rather base my use [of health-tracker devices] on what I have heard from others than being the guinea pig. [...] I would like to see a lot of that other experience.*" (P121)

6.7.5 Alternative options for achieving the decision maker's goal.

Environment > Alternative options for achieving the decision maker's goal

In addition to evaluating *whether a particular system, device, or app really needs the requested data* to perform its functionalities (see §6.2.2), a decision maker may also consider the existence and availability of **alternative options for achieving their goal**, outside the system in question: "*I do not use Twitter or email much at all. I prefer [my healthcare provider], for instance, to send me a postcard and/or a phone call [for an appointment reminder].*" (P69) Sometimes important tasks must be done online if no alternatives exist: "*I don't think I would ever want to put any information [on the computer] like banking or even medical stuff, unless it was unavoidable.*" (P1)

The comparisons of alternatives might be between different online scenarios or between online and offline scenarios. In particular, decision-makers may choose alternative means based on whether they generally prefer to communicate in person, or at least via a maximally personal channel: "*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.* " (P32)

⇆ Connections and Trade-Offs ⇆

Participants evaluate each alternative sharing scenario along the same dimensions. The *Alternative options* factor involves considering whether alternatives exist, and may also involve comparing parallel models of each alternative with respect to particular factors. For example, participants weighed the relative desirability of using different systems or services in terms of *monetary cost* (see §6.6.2) or the time and *effort required to use them* (see §6.6.1): "*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 a lot.*" (P22)

Participants also mentioned comparing the *likelihood* and *extent of benefits* (see §6.4.2, §6.4.3), sometimes with reference to special *circumstances that might increase the need for sharing* (see §6.1.2), as well as the *likelihood* and *severity of risks* associated with different scenarios (see §6.5.1, §6.5.2): "*I don't do any monetary transactions online at all. [...] I just don't think [online shopping] 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)

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

7.1.1 Comparisons with existing theoretical frameworks. For the most part, our model is compatible with each of the theories reviewed in §2.2, 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 broad enough in scope to be applicable to a wide variety of situations, yet sufficiently detailed regarding the particular contextual factors that may affect information sharing decision-making to be successfully operationalizable.

In its focus on contextual factors, our model shares the most similarities with the Theory of Privacy as Contextual Integrity (CI) [83, 85]. 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 the norm-based privacy expectations they give rise to, constitute one 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 have been some attempts to empirically study the impact of certain transmission principles on information-sharing attitudes and intentions [61, 62, 102], to the best of our knowledge, no one has offered a systematic theoretical framework for transmission principles. In addition, our granular description of factors can help to systematically evaluate existing systems to identify potential points of intervention, and provide an accessible starting point for designing new systems that (for example) better respect contextual norms (see §7.2).

As with CI, our model is compatible with Communication Privacy Management Theory [64, 90, 91] and Altman's Boundary Regulation Theory [6, 7], but has a different scope. Both of these approaches focus in-depth on the balance between goals (avoiding intrusion when sharing information publicly vs. avoiding loneliness when keeping 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 may have, such as monitoring health or protecting loved ones from worry.

Our findings include factors pertinent to protection self-efficacy, and perceptions and severity of privacy threats like those outlined in Protection Motivation Theory [98] and Technology Threat Avoidance Theory [57]. Similarly, benefits and costs, central to the Privacy Calculus (PC) approach [35, 36], 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, such as trust in recipients' intentions or technological self-efficacy, that recognize that decision makers are not necessarily fully rational agents.

In sum, some of our factors and dimensions align with elements that are explained in depth by other models and frameworks, though it is broader and more comprehensive. This is partially due to the fact that we addressed a different research question: we seek to identify and empirically account for as many factors as possible that users deliberate about in making information-sharing decisions, rather than to focus on analysing particular aspects. 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. 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:

- Advance understanding of the complexity of information-sharing decision making, including the relations between contextual factors, and their valence and relative importance.
- Account for contextual factors during systematic reviews of literature and empirical evidence about data sharing preferences and behaviors.
- Design empirical studies (survey instruments, interview protocols, vignette scenarios, experimental design, etc.) to analyse and compare different populations of users' attitudes, preferences, decision making, and behaviors, while systematically accounting for the contextual factors and validating their effects.
- 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. In particular, this work can inform research on improving the transparency of data flows between older adults and caregivers while respecting older adults' privacy preferences, and desire for agency and control over their own information. 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. Interventions that account for older adults' existing decision-making practices—especially the effects of differential technology acceptance and self-efficacy—can better prepare them to independently protect their online privacy and security. (For more suggestions for awareness and education programs and outreach targeted to older adults, see Frik et al. [39]).
- Design and test interventions, and evaluate existing ones, for educating system designers and developers about improving transparency and control. Our work can offer particular insights about design of products for older adults and aged care, as it is based in detailed analysis of their opinions and preferences about information sharing. Such research can provide or improve practical tools for designing usable systems that empower informed choice, meet users' expectations, address concerns, and allow them to tune systems to their preferences (see §7.2.2).
- Evaluate existing policies and regulations about data transparency, protection, and control, and inform improvements in regulation enforcement and control mechanisms.

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. 63, 80]). 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 systematically validate the model with other audiences (e.g. younger users, medical professionals and caregivers, seniors' family members, people from other countries and with various cultural backgrounds). As well as examining differences between those groups in weighting of factors, we may potentially identify new factors—or relationships between factors—that are less pertinent to older adults in the US but may be more pertinent to other groups. We will also compare how the factors affect preferences and decisions about sharing information via (or with) different types of 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 and others' theoretical and empirical work (such as that discussed in §2.1.2, §2.2, and §7.1.1), we can begin accounting for how people weigh the different contextual factors in practice, including differences in these practices between different age groups.

Finally, future research may include a database aggregating this knowledge, including theoretical and empirical evidence, and best practices on each of the parameters in our model, to make relevant information searchable for researchers, practitioners, system designers, and policymakers.

7.2 Practical Implications and Proposed Interventions

As we noted above, we did not observe unequivocal opinions amongst our participants; decisions were usually conditional. We believe that quantifying our model (as described in §7.1.3) will provide useful mapping and insights into how decisions depend on the factors, how those factors are weighted, and whether they have strong valences. Such mapping in turn will help inform technology design.

7.2.1 Implications of the model for product design. The complexity and context-dependency of data-sharing preferences and expectations means there is no one best way to design a product that will make all older adults feel comfortable sharing data with it. However, a reasonable first step is to build trust with the user by being transparent, clear, and honest about the *goals of data collection and use* and about *recipients* with whom the data will be shared, as those are two main factors mentioned by nearly all of our participants (see §6.6.6). (This is in line with previous work showing trust is one of the main conditions for older adults' adoption of IoT [25, 31, 39, 71].)

Our participants expressed an extensive *desire for control* over personal information (see §6.1.1), and when prompted in the interview situation, they came up with very specific, fine-grained preferences about recipients, goals, locations, and circumstances. The challenge for designers is to provide sufficient specificity without making the controls too complicated and unusable.

As our sample size is insufficient to quantify the prevalence and importance of specific factors and sub-factors, we do not provide specific recommendations about which factors should be prioritized for user controls. Future empirical research and experimentation is required to design and test optimal control mechanisms.

7.2.2 Future work: Proposed interventions.

Tools for designers/developers. Our model can offer developers and designers guidance in navigating contextual complexity and evaluating the potential impact of particular contextual factors on users' reactions to products that they design. Based on the factors in our model, 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. [26, 38, 110]). Prompts such as "What formats are data *currently* collected in? What other data formats could *potentially* achieve the same goal using less identifiable information?" would help designers and developers systematically evaluate or compare systems and prototypes along the dimensions/factors/sub-factors of our model.

Outside of industry, prompts could be used in research and in-class activities to evaluate and compare information-sharing preferences and behaviors across various scenarios.

Our model may also provide useful guidance in selecting features for training machine learning algorithms (e.g., similar to SPISM [16]) that would automate 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.

Consumer education. We plan to develop and test a curriculum geared specifically to older adults that teaches best security and privacy practices. We will customise the materials to better address specific needs and concerns observed in our and prior work, provide verified information on factors that affect older adults' sharing decisions (e.g., probabilities and consequences of security risks), and tailor accessibility of the materials for the cognitive and physical abilities of the elderly.

Additionally, to address the effects of factors such as *technology self-efficacy*, *understanding of the sharing scenario* and *knowledge of the specific data flows and mechanisms involved*, we plan to examine comprehension of information sharing, and of privacy and security vocabulary, among older adults and younger populations. After testing comprehension of language used in permissions requests and in privacy policies/disclosures, we will ask respondents to propose alternatives for unclear terms. We will map this mismatches into guidelines to improve effective communication about privacy and security between technologists and lawyers who design policies and interfaces and different socio-demographic groups of users, including older adults, along the factors outlined in the model.

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 relative to the general population. Therefore, studying the privacy decision-making processes of elderly people, including non-users, will help us understand the concerns surrounding emerging technologies across more general populations, and discover deeper insights that may be overlooked in studies with typical user communities. Future research is called for to test whether the model is valid for other specific user groups, as well as for the general population.

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, Noura Alomar, 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 and the 2020 Workshop on the Economics of Information Security (WEIS) for comments on the model, and anonymous reviewers for WEIS and TOCHI for suggestions about the paper. This work was supported by the Center for Long-Term Cybersecurity at UC Berkeley, U.S. National Security Agencycontract H98230-18-D-0006, National Science Foundation grants CNS-1514211 and CNS-1528070, and the Rose Foundation for Communities and the Environment.

REFERENCES

[1] Noura Abdi, Xiao Zhan, Kopo M. Ramokapane, and Jose Such. 2021. Privacy Norms for Smart Home Personal Assistants. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3411764.3445122

[2] 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.

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

[4] 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.

[5] 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

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

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

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

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

[10] 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.

[11] 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

[12] 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.

[13] 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.

[14] 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

[15] Clara Berridge and Terrie Fox Wetle. 2020. Why Older Adults and Their Children Disagree About In-Home Surveillance Technology, Sensors, and Tracking. *The Gerontologist* 60, 5 (July 2020), 926–934. https://doi.org/10.1093/geront/gnz068

[16] 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.

[17] 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).

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

[19] 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

[20] Alison Burrows, David Coyle, and Rachael Gooberman-Hill. 2018. Privacy, boundaries and smart homes for health: An ethnographic study. *Health & Place* 50 (2018), 112–118. https://doi.org/10.1016/j.healthplace.2018.01.006

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

[22] BD Carpenter and S Buday. 2007. Computer use among older adults in a naturally occurring retirement community. *Computers in Human Behavior* 23, 6 (2007), 3012–3024.

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

[24] 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.

[25] 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.

[26] 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.

[27] Raymundo Cornejo, Robin Brewer, Caroline Edasis, and Anne Marie Piper. 2016. Vulnerability, sharing, and privacy: Analyzing art therapy for older adults with dementia. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. 1572–1583.

[28] 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.

[29] 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).

[30] 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).

[31] 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.

[32] Lorrie Faith Cranor. 2008. A Framework for Reasoning about the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security (UPSEC'08)*. USENIX Association, USA, Article 1, 15 pages.

[33] 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.

[34] 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).

[35] 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.

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

[37] Kerry Dobransky and Eszter Hargittai. 2016. Unrealized potential: Exploring the digital disability divide. *Poetics* 58 (2016), 18–28.

[38] 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.

[39] 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.

[40] 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*.

[41] Vaibhav Garg, L. Jean Camp, Lesa Lorenzen-Huber, Kalpana Shankar, and Kay Connelly. 2014. Privacy concerns in assisted living technologies. *annals of telecommunications - annales des tÃľlÃľcommunications* 69, 1 (Feb. 2014), 75–88. https://doi.org/10.1007/s12243-013-0397-0

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

[43] Frederic Gerdon, Helen Nissenbaum, Ruben L. Bach, Frauke Kreuter, and Stefan Zins. 2021. Individual Acceptance of Using Health Data for Private and Public Benefit: Changes During the COVID-19 Pandemic. *Harvard Data Science Review* (April 2021). https://doi.org/10.1162/99608f92.edf2fc97

[44] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J. Wisniewski, Xinru Page, and Bart Knijnenburg. 2021. To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In *Proceedings of the 2021 ACM CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, Article 686, 14 pages. https://doi.org/10.1145/3411764.3445204

[45] 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.

[46] Galen A Grimes, Michelle G Hough, and Margaret L Signorella. 2007. Email end users and spam: Relations of gender and age group to attitudes and actions. *Computers in Human Behavior* 23, 1 (2007), 318–332.

[47] Michael Haight, Anabel Quan-Haase, and Bradley A Corbett. 2014. Revisiting the digital divide in Canada: The impact of demographic factors on access to the Internet, level of online activity, and social networking site usage. *Information,*

Communication & Society 17, 4 (2014), 503–519.

[48] 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

[49] Michelle G Hough. 2004. Exploring elder consumers interactions with information technology. *Journal of Business & Economics Research (JBER)* 2, 6 (2004).

[50] 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.

[51] Sydney Jones and Susannah Fox. 2009. *Generations online in 2009.* Technical Report. Pew Internet & American Life Project, Washington, DC.

[52] 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).

[53] 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.

[54] 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.

[55] Hosub Lee and Alfred Kobsa. 2016. Understanding user privacy in Internet of Things environments. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT).* 407–412. https://doi.org/10.1109/WF-IoT.2016.7845392

[56] 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

[57] 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

[58] 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.

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

[60] 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.

[61] 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.*

[62] 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.

[63] 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.

[64] 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

[65] 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.

[66] Nora McDonald, Alison Larsen, Allison Battisti, Galina Madjaroff, Aaron Massey, and Helena Mentis. 2020. Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges. In *Sixteenth Symposium on Usable Privacy and Security ({SOUPS} 2020).* 99–110.

[67] Nora McDonald and Helena M Mentis. 2021. Building for âĂŸWeâĂŹ: Safety Settings for Couples with Memory Concerns. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems.* 1–11.

[68] 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.

[69] A. K. M. Nuhil Mehdy, Michael D. Ekstrand, Bart P. Knijnenburg, and Hoda Mehrpouyan. 2021. *Privacy as a Planned Behavior: Effects of Situational Factors on Privacy Perceptions and Plans.* Association for Computing Machinery, New York, NY, USA, 169âĂŞ178. https://doi.org/10.1145/3450613.3456829

[70] 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/

[71] 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.

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

[73] Helena M Mentis, Galina Madjaroff, Aaron Massey, and Zoya Trendafilova. 2020. The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–19.

[74] 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).

[75] Mainack Mondal, Zhuo Lin, Tamara Babaian, Xinru Page, and Blase Ur. [n. d.]. Using Long-Lived Facebook Accounts to Understand Implicit Norms of Consent in Contextual Integrity. Presentation at the 2nd Symposium on Applications of Contextual Integrity, August 19–20, 2019, Berkeley, CA, USA.

[76] 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

[77] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–24.

[78] 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.

[79] 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)*. 399–412.

[80] 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

[81] 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.

[82] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 ACM CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1âĂŞ11. https://doi.org/10.1145/3290605.3300579

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

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

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

[86] Helen Nissenbaum. 2019. Contextual Integrity Up and Down the Data Food Chain. *Theoretical Inquiries in Law* 20, 1 (Jan. 2019), 221–256. https://doi.org/10.1515/til-2019-0008 Publisher: De Gruyter.

[87] 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.

[88] 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)*.

[89] Stacey Pereira, Jill Oliver Robinson, Hayley A. Peoples, Amanda M. Gutierrez, Mary A. Majumder, Amy L. McGuire, and Mark A. Rothstein. 2017. Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLOS ONE* 12, 9 (Sept. 2017), e0184525. https://doi.org/10.1371/journal.pone.0184525 Publisher: Public Library of Science.

[90] 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.

[91] 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

[92] 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.

[93] Javad Pool, Saeed Akhlaghpour, Farhad Fatehi, and Leonard C. Gray. 2022. Data privacy concerns and use of telehealth in the aged care context: An integrative review and research agenda. *International Journal of Medical Informatics* 160 (April 2022). https://doi.org/10.1016/j.ijmedinf.2022.104707

[94] Erika Shehan Poole, Marshini Chetty, Rebecca E Grinter, and W Keith Edwards. 2008. More than meets the eye: transforming the user experience of home network management. In *Proceedings of the 7th ACM conference on Designing interactive systems*. 455–464.

[95] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 739–748.

[96] Lee Rainie and Maeve Duggan. 2016. *Privacy and Information Sharing*. Technical Report. Pew Research Center. http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/ Accessed: 16 February 2022.

[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] Sergio Sayago and Josep Blat. 2010. Telling the story of older people e-mailing: An ethnographical study. *International Journal of Human-Computer Studies* 68, 1-2 (2010), 105–120.

[100] Statista. 2019. Percentage of internet users in the United States who use e-mail as of November 2019, by age group. (2019). Accessed 14 January 2022: https://www.statista.com/statistics/271501/us-email-usage-reach-by-age/.

[101] 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

[102] 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.

[103] 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.

[104] 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.

[105] 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.

[106] Jessica Vitak and Michael Zimmer. 2020. More Than Just Privacy: Using Contextual Integrity to Evaluate the Long-Term Risks from COVID-19 Surveillance Technologies. *Social Media + Society* 6, 3 (July 2020). https://doi.org/10.1177/2056305120948250 Publisher: SAGE Publications Ltd.

[107] 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.

[108] 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.

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

[110] 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.

[111] 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).

[112] 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.

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

[114] 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.

[115] 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.

[116] 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

[117] 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) Desire for agency and control
  - (ii) Circumstances that make the decision maker feel especially vulnerable to certain risks
  - (iii) Personal experiences with privacy or security violations
  - (iv) *Environment > Norms about appropriate or usual information sharing*
- (b) **Technology acceptance** (§6.1.2)
  - (i) Technology self-efficacy
    - *Decision Maker > Perceived understanding of the sharing scenario*
  - (ii) Circumstances that increase the need to share certain information
- (c) **Perceived understanding of the sharing scenario** (§6.1.3)
  - (i) Past experiences with similar or related data sharing scenarios
  - (ii) Knowledge of the specific data flows and mechanisms involved
  - (iii) *Decision Maker > Technology Acceptance > Technology self-efficacy*
  - (iv) *Environment > Stories about privacy and information sharing*

DATA

- (a) **Relevance to the recipient/goal** (§6.2.1)
- (b) **Whether the data is necessary to the goal** (§6.2.2)
- (c) **Amount/extent** (§6.2.3)
  - (i) Accumulation of data over time
    - Continuity of data collection
    - *System > Data retention*
  - (ii) Granularity/specificity
  - (iii) Data format and 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 about privacy and information sharing*
    - Assessment based on appearances
  - (ii) Evaluation of recipients' judgment and competence/ability
- (b) **Degree of removal** (§6.3.2)
- (c) **Recipients' potential reactions** (§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) Likelihood 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) *Recipients > Trust in recipients*

(c) **Extent of benefits** (§6.4.3)

(i) Importance or added value for the party who accrues the benefits

(ii) Urgency/time sensitivity of receiving the benefits

RISKS

(a) **Perceived likelihood of negative consequences occurring** (§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
- *Recipients > Trust in recipients*
- *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 about privacy and information sharing*

(iii) Potential inferences from the data

(iv) Reusability of the data across contexts

(v) *Data > Amount/extent*

(vi) *System > Data retention*

(vii) *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 using the system** (§6.6.1)

(i) Intrusiveness of the data collection process

(ii) Effort required to use the system

- *Decision Maker > Technology acceptance > Technology self-efficacy*

(b) **Cost of using the system** (§6.6.2)

(c) **Data retention** (§6.6.3)

(d) **Connection to the Internet** (§6.6.4)

- Transmission channel
- Hosting

(e) **Human involvement** (§6.6.5)

(f) **Transparency about data flows** (§6.6.6)

(g) **Ability to control data flows and mitigate or protect against risks** (§6.6.7)

(i) Effort required to control/protect/mitigate

- *Decision maker > Technology acceptance > Technology self-efficacy*

(ii) Cost of control/protection/mitigation

(iii) Likely effectiveness of the means of control/protection/mitigation

- *Evaluation of recipients' judgment and competence/ability*

ENVIRONMENT

(a) **Norms about appropriate or usual behavior** (§6.7.1)
  (i) Laws about behavior

(b) **Norms about appropriate or usual information sharing** (§6.7.2)

(c) **Laws about information sharing** (§6.7.3)

(d) **Stories about privacy and information sharing** (§6.7.4)
  (i) Media stories
  (ii) Past experiences of the decision maker's close connections

(e) **Alternative options for achieving the decision maker's goal** (§6.7.5)