



Titre: Investigating Technology Users' Privacy Attitudes and Motivation to
Title: Attend to Information Privacy

Auteur: Varun Kevin Shiri
Author:

Date: 2024

Type: Mémoire ou thèse / Dissertation or Thesis

Référence: Shiri, V. K. (2024). Investigating Technology Users' Privacy Attitudes and
Citation: Motivation to Attend to Information Privacy [Mémoire de maîtrise, Polytechnique
Montréal]. PolyPublie. <https://publications.polymtl.ca/59169/>

 **Document en libre accès dans PolyPublie**
Open Access document in PolyPublie

URL de PolyPublie: <https://publications.polymtl.ca/59169/>
PolyPublie URL:

**Directeurs de
recherche:** Jinghui Cheng
Advisors:

Programme: génie informatique
Program:

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

**Investigating Technology Users' Privacy Attitudes and Motivation to Attend to
Information Privacy**

VARUN KEVIN SHIRI

Département de génie informatique et génie logiciel

Mémoire présenté en vue de l'obtention du diplôme de *Maîtrise ès sciences appliquées*
Génie informatique

August 2024

POLYTECHNIQUE MONTRÉAL

affiliée à l'Université de Montréal

Ce mémoire intitulé :

**Investigating Technology Users' Privacy Attitudes and Motivation to Attend to
Information Privacy**

présenté par **Varun Kevin SHIRI**

en vue de l'obtention du diplôme de *Maîtrise ès sciences appliquées*

a été dûment accepté par le jury d'examen constitué de :

Zohreh SHARAFI, présidente

Jinghui CHENG, membre et directeur de recherche

Martin ROBILLARD, membre externe

DEDICATION

*To my grandmother,
you are my greatest inspiration. . .*

*À ma grand-mère,
vous êtes ma plus grande inspiration. . .*

ACKNOWLEDGEMENTS

The culmination of this journey has been the collective effort of a number of individuals to whom I express my deepest and heartfelt gratitude. Firstly, I am immensely grateful to my research director, Prof. Jinghui Cheng, who has been the best supervisor I could have asked for. His constant guidance, encouragement, empathy and understanding at every step of my journey has motivated me to better my best. Similarly, I am extremely thankful to Prof. Jin Guo from McGill University, who, along with Prof. Cheng, has been my mentor and guide throughout my master's journey. They always went above and beyond their duty to ensure that I had the needed support and resources to progress in my research. Without their personal interest and deep involvement in my research work, as well as my personal welfare, it would have been impossible to accomplish what I have today.

I cannot thank my dearest family enough, as they are the very reason I undertook this journey. My immense gratitude goes to my sister—my inspiration and lifeline—who started the journey here alone so that I could have the privilege of having a family member to support me when I arrived. From the bottom of my heart, I express my gratitude to my wonderful mother for her unconditional love and support. I had the rare privilege of starting my journey in this country with her by my side. Without her sacrifices and unwavering support, I would not have been able to tread this path. I am also indebted to my father, my biggest pillar and mentor, who has molded me into the person I am. His commitment, dedication and sacrifices have inspired me to push forward. He has helped me overcome every obstacle along the way and maintain a positive outlook throughout this journey. My heartfelt gratefulness goes to my aging grandmother, who has been my unfailing supporter and well-wisher. The sterling woman she is and the similar journey she embarked on back in the day are my greatest sources of inspiration.

I would also like to extend my gratitude to all my fellow members in the HCD Lab for their help and encouragement. Our interchange of ideas and knowledge has helped me grow and learn new things. I cherish the moments we shared together and I wish for their continued success. I would like to especially thank Maggie Xiong, my collaborator and co-author in my research, whose help and contributions have been essential to the success of our works. Finally, I am grateful to the jury for dedicating the time and effort to carefully review my thesis.

RÉSUMÉ

Dans l'environnement technologique actuel, les utilisateurs se retrouvent souvent dans une position vulnérable lorsqu'il s'agit de protéger la confidentialité de leurs données. Par conséquent, il est crucial de sensibiliser les utilisateurs à la confidentialité et de leur donner les moyens de prendre des décisions concrètes quant à la confidentialité de leurs informations. Les efforts existants se sont largement concentrés sur la présentation de la politique de confidentialité et n'ont pas réussi à relever systématiquement le défi radical de la motivation des utilisateurs à initier une sensibilisation à la confidentialité. Cette thèse vise à fournir une analyse approfondie de la sensibilisation et des perspectives des utilisateurs en matière de confidentialité et à tenter de repenser le moyen de communication des informations sur la confidentialité aux utilisateurs afin de renforcer la motivation à interagir avec ces informations importantes.

Dans la première partie de la thèse, nous examinons le comportement collectif de recherche d'informations et de création de sens des utilisateurs en matière de confidentialité dans les forums de questions-réponses en ligne afin de tirer des informations précieuses sur leurs perspectives en matière de confidentialité et de suggérer des moyens de leur permettre de prendre un meilleur contrôle. Nous abordons cela en analysant un échantillon aléatoire de 313 questions liées à la confidentialité et leurs réponses sur Quora. Nos résultats ont mis en évidence la complexité de la confidentialité de données du point de vue des utilisateurs, englobant un large éventail de sujets interconnectés. Nous avons également constaté que la plupart des questions visaient des opinions personnelles et que de nombreuses réponses étaient imprégnées d'émotions et d'histoires personnelles ; ceux-ci indiquent que la confidentialité est une expérience personnelle et subjective pour les utilisateurs de technologie. Nos recherches nous ont permis d'identifier les opportunités permettant aux développeurs d'intégrer les points de vue des utilisateurs sur la confidentialité dans leurs pratiques de développement. Il a également souligné l'importance de favoriser les échanges communautaires pour mieux aider les utilisateurs à protéger leurs données privées et la nécessité d'établir des exemples industriels pour endiguer la vague de pratiques invasives en matière de confidentialité.

Dans la deuxième partie de la thèse, nous étudions une approche de conception basée sur la théorie pour motiver les utilisateurs à veiller à la confidentialité de leurs informations. À cette fin, nous avons exploité la théorie de la motivation de protection (Protection Motivation Theory ou PMT) pour proposer des idées de conception et des catégories dédiées à motiver les utilisateurs à interagir avec les informations liées à la confidentialité de données. En

utilisant ces idées de conception, nous avons créé un prototype conceptuel, améliorant la page produit actuelle de l'App Store. Les résultats d'une expérience en ligne et d'entretiens de suivi ont montré que notre conception a efficacement motivé les participants à s'occuper des problèmes de confidentialité, augmentant à la fois l'évaluation de la menace (threat appraisal) et l'évaluation de l'adaptation (coping appraisal), deux facteurs principaux du PMT. Nos travaux ont indiqué qu'une conception efficace devrait envisager de combiner les composants PMT, de calibrer le contenu de l'information et d'intégrer d'autres éléments de conception, tels que les repères visuels et la familiarité de l'utilisateur.

Dans l'ensemble, cette thèse considère une approche centrée sur l'utilisateur (de bas en haut) pour naviguer dans le paysage complexe de la confidentialité, complétant les efforts actuels principalement centrés sur la réglementation (de haut en bas). En nous concentrant sur les points de vue des utilisateurs et sur l'aspect motivationnel de la communication relative à la confidentialité, nous visons à donner aux individus les moyens de mieux contrôler leurs données privées lorsqu'ils interagissent avec des applications logicielles.

ABSTRACT

In the current technology environment, users often find themselves in a vulnerable position when it comes to protecting their privacy. Therefore, raising users' privacy awareness and empowering them to make concrete decisions to attend to their information privacy is crucial. Existing efforts largely focused on privacy policy presentation and failed to systematically address a radical challenge of user motivation for initiating privacy awareness. This thesis aims to provide an in-depth analysis of users' privacy awareness and perspectives and to investigate redesigning the medium of communicating privacy information to users to enhance motivation to engage with this important information.

In the first part of the thesis, we examine users' collective information-seeking and sense-making behavior towards privacy in online Q&A forums to draw valuable insights into their privacy perspectives and suggest ways to empower them to take better control. We approach this by analyzing a random sample of 313 privacy-related questions and their answers on Quora. Our results highlighted the complexity of privacy from the users' perspective, encompassing a wide range of interconnected topics. We also found that most of the questions sought personal opinions and many answers were infused with emotions and personal stories; these indicated that privacy is a personal, subjective experience for technology users. Our research enabled us to pinpoint opportunities for developers to incorporate user perspectives on privacy into their development practices. It also emphasized the significance of fostering community exchange to better support users in attending to their privacy and the need to establish industrial exemplars to stem the tide of invasive privacy practices.

In the second part of the thesis, we investigate a theory-driven design approach to motivate users to attend to their information privacy. We leveraged the Protection Motivation Theory (PMT) to propose design ideas and categories dedicated to motivating users to engage with privacy-related information. Using these design ideas, we created a conceptual prototype, enhancing the current App Store product page for a hypothetical fitness tracking app. Results from an online experiment and follow-up interviews showed that our design effectively motivated participants to attend to privacy issues, raising both the threat appraisal and coping appraisal, two main factors in PMT. Our work indicated that effective design should consider combining multiple motivational factors, calibrating information content, and integrating design elements such as visual cues and user familiarity.

Overall, supplementing the currently predominant regulation-centered (top-down) efforts, this thesis considers a user-centered (bottom-up) approach to navigating the complex pri-

vacy landscape. By focusing on users' perspectives and the motivational aspect of privacy communication, we aim to empower individuals to take better control of their privacy when interacting with software applications.

TABLE OF CONTENTS

DEDICATION	iii
ACKNOWLEDGEMENTS	iv
RÉSUMÉ	v
ABSTRACT	vii
TABLE OF CONTENTS	ix
LIST OF TABLES	xii
LIST OF FIGURES	xiii
LIST OF SYMBOLS AND ACRONYMS	xiv
CHAPTER 1 INTRODUCTION	1
1.1 Context and Motivation	1
1.2 Research Objectives and Approach	2
1.3 Thesis Outline	3
CHAPTER 2 LITERATURE REVIEW	4
2.1 Investigating Users' Privacy Attitude	4
2.2 Users' Challenges Concerning Privacy Policy	5
2.3 Design Solutions to Enhance Privacy Policies	6
2.4 Understanding How Developers Approach Privacy	8
CHAPTER 3 ANALYSIS OF USER PRIVACY DISCUSSIONS IN ONLINE FORUMS	10
3.1 Introduction	10
3.2 Previous Studies of Online Community on Quora	11
3.3 Methods	12
3.3.1 Data Collection	12
3.3.2 Data Analysis	12
3.3.3 Limitations	13
3.4 Results: Privacy Topics	14
3.4.1 Privacy Protection Strategies	14

3.4.2	Privacy Risks and Dangers	19
3.4.3	Privacy in Organizations	22
3.4.4	Privacy Laws, Rules and Regulations	23
3.4.5	Other Topics	24
3.4.6	Relationship Between Question Topics and Response Topics	25
3.5	Results: Types of Questions	25
3.5.1	Opinion	26
3.5.2	Factual	26
3.5.3	Instruction or Guidance	27
3.5.4	Relationship Between Question Types and Question Topics	27
3.6	Results: Characteristics of Responses	28
3.6.1	Emotional Arousal	28
3.6.2	Example	29
3.6.3	External Source	29
3.6.4	Personal Experience	30
3.6.5	Relationship Between Response Characteristics and Response Topics	30
3.7	Discussion	30
3.7.1	The Complexity of Privacy Topics	31
3.7.2	The Overwhelmed and Often Helpless Users	32
3.7.3	Comparing Developer and End User Privacy Discussions in Online Forums	33
3.7.4	Implications to Practice and Research	35
3.8	Conclusion	35
CHAPTER 4	THEORY-DRIVEN DESIGN STUDY	37
4.1	Introduction	37
4.2	A Narrative Literature Review on the Design for Privacy Policies	38
4.2.1	Discussion and Reflection	39
4.3	The Protection Motivation Theory	40
4.3.1	Protection Motivation Theory	41
4.3.2	Applications of PMT in HCI, Security and Privacy	42
4.4	Design Process	43
4.4.1	Case Study Selection	43
4.4.2	Design Ideation	44
4.4.3	Design Iterations	44
4.5	Final Design	46

4.5.1	Privacy FAQ	46
4.5.2	Privacy Rating	46
4.5.3	Privacy Tutorial	48
4.5.4	Privacy Prompt	48
4.5.5	Privacy Reviews	48
4.6	User Study Methods	48
4.6.1	Online Experiment	49
4.6.2	Interview	52
4.7	User Study Results	53
4.7.1	Rating on PMT Dimensions	53
4.7.2	User Feedback on the Control Design	54
4.7.3	User Feedback on the Treatment Design	56
4.8	Discussion	60
4.8.1	Design Considerations for Motivating Users to Attend to Privacy . .	61
4.8.2	Practical Implications of Our Design	62
4.8.3	Limitations and Future Work	64
4.9	Conclusion	65
CHAPTER 5	CONCLUSION	66
5.1	Summary of Works	66
5.2	Limitations & Future Work	67
REFERENCES		69

LIST OF TABLES

Table 4.1	Papers included in the narrative literature review and the extracted challenge and design categories.	40
Table 4.2	PMT components illustrated through an analogy of quitting smoking from the previous PMT literature [1] and when adapted to motivate users to attend to privacy.	41
Table 4.3	Design categories and ideas emerged from the design ideation phase .	45
Table 4.4	Participant demographics of the online experiment	50
Table 4.5	Final PMT statements for online experiment	51
Table 4.6	Participant demographics of the interview	53

LIST OF FIGURES

Figure 3.1	Frequency of privacy topics in questions and responses	15
Figure 3.2	Percentages of questions in each privacy topic answered with responses touching on each topic	25
Figure 3.3	Percentages of questions in each privacy topic that were asked with each question type	27
Figure 3.4	Percentages of responses containing each privacy topic identified with each response characteristic	31
Figure 4.1	Primary features to motivate privacy consideration in our final design, including ① privacy FAQ, ② rating on privacy practice of the app, ③ a short tutorial on customizable privacy options, ④ a prompt for users to review privacy FAQ before downloading the app, and ⑤ user reviews related to privacy.	47
Figure 4.2	Participant ratings for PMT statements. The stars indicate significant differences between the control and the treatment conditions (** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$).	54

LIST OF SYMBOLS AND ACRONYMS

GDPR	General Data Protection Regulation
OECD	Organisation for Economic Co-operation and Development
PMT	Protection Motivation Theory

CHAPTER 1 INTRODUCTION

1.1 Context and Motivation

In today’s technological landscape, every user inevitably encounters a plethora of applications and services that produce, collect, analyze, and disseminate their personal data. While some of these practices can be useful, aiming at enhanced user experiences, others do not directly benefit users, gearing towards profiting from targeted advertisements or other financial avenues. Regardless of the intention of the app and service providers, users should be provided with opportunities to understand and have control over the ways their personal data is handled by those applications and services. Technology users, however, are in a precarious position when it comes to protecting their privacy. The fundamental problem is that they often have limited options other than those given by the technology developers and service providers, who, in turn, face conflicting interests between protecting users’ privacy and generating profit from their data. As users encounter multiple challenges navigating the multitude of technologies integral to their daily lives, it becomes increasingly imperative to investigate ways to empower users to take control of their privacy in today’s technology environment. From a user-centered perspective, this investigation should start with an understanding of how users currently acquire information and knowledge to assess privacy risks and protect their information privacy. Then, user-oriented solutions should be explored to support technology users to move beyond mere worries and enable meaningful actions for self-protection. This effort will eventually enforce responsible innovation of technology providers.

Over time, many privacy-related regulations and guidelines have been implemented, such as the Privacy Act in Canada [2], the OECD guidelines [3], and more recently, GDPR [4]. These regulations and guidelines predominantly focus on regulating the conduct of companies and developers, including compelling them to communicate their privacy practices to users primarily through privacy policies. As such, the privacy policy has become an essential informational interface between users and the privacy practice of the app and service developers [5]. A privacy policy, however, is far from an ideal interface for communicating privacy practices to users [6–8]. Previous research has established that: (1) privacy policies are often lengthy [7, 9–12], ambiguous [13–16], filled with jargon [9, 15, 17], and constantly evolving [11, 18]; and (2) users’ perceptions of privacy policy are largely negative, which precludes users from being motivated enough to understand the privacy practices and protect their privacy [10, 13]. While these two types of challenges are closely related, existing design solutions mostly focus on the first type of challenge (e.g., [14]), leaving the critical aspect of

user motivation largely unaddressed. We argue that HCI researchers need to extend their focus to motivating users to actively seek and act on privacy-related information and empower users to protect their privacy.

1.2 Research Objectives and Approach

Our primary focus in this thesis is **to bridge the motivational gap between users' privacy concerns and actions through (1) understanding users' current privacy perspectives and attitudes and (2) effective redesign of the privacy informational interface between users and the technology providers**. As mentioned before, to help users navigate complex privacy choices and increase their privacy awareness, we should start with an understanding of how users currently acquire such information and knowledge. In our initial exploration, we discovered that online discussion forums serve as an important venue for users to exchange their perspectives, firsthand experiences, and advice regarding various privacy-related subjects. Therefore, a study of user discussions on such platforms can help us gain insights into their privacy perspectives and attitudes. These insights can be useful in redesigning the informational interface to effectively communicate the privacy practice of apps and services with users, particularly when such information becomes pertinent to the user's interests and rights. Furthermore, our own experience and informal discussions with other users indicate that many users still do not care about privacy or neglect it when making concrete app usage decisions, even when the information is distilled into a concise format (e.g., as privacy labels in app stores). The potential impact of redesigning the privacy policy representation can be substantially enhanced by considering this motivational issue as a primary design objective.

To achieve our objectives, we conducted the following two studies.

- In the first study, we focused on understanding users' current privacy attitudes by analyzing a random sample of 313 privacy-related discussions retrieved from the popular Q&A site Quora. Specifically, we aimed to extract the following information from the questions and answers: (1) the range of privacy topics users discuss on this question-and-answer platform, (2) the type of information users sought in privacy-related questions, and (3) the characteristics of the answers to these questions. We followed an inductive coding approach to extract this information. Our analysis revealed the multifaceted nature of privacy for users, with questions spanning a broad spectrum of interrelated topics. We also drew parallels between users' and developers' discussions around privacy in online forums, revealing opportunities for developers to integrate

users’ privacy concerns in the development lifecycle.

- In the second study, we adopted a theory-driven design approach [19], leveraging the Protection Motivation Theory (PMT) [20, 21] to propose design ideas and categories aimed at increasing users’ motivation to engage with privacy-related information. These design propositions motivated the creation of a conceptual prototype of the App Store product page for a hypothetical fitness app. To assess the impact of our design ideas, we conducted a two-phase user study involving an online experiment followed by a set of interviews, where users compared our conceptual design prototype with the existing App Store interface. Our results showed that our design effectively motivated participants to attend to privacy issues, particularly raising their sensitivity to privacy threats. Further, we contribute important design considerations and implications to address the motivational aspect of users’ privacy awareness and actions.

1.3 Thesis Outline

The rest of the thesis is organized as follows. Chapter 2 outlines the previous literature focusing on users’ privacy attitudes and challenges, design solutions to address the problems with privacy policies, and developers’ privacy considerations. Chapter 3 presents an empirical study of privacy-related discussions on the Q&A forum Quora, aiming to provide a concrete understanding of the various layers of users’ privacy perceptions and concerns. Building on the observations from our literature review in Chapter 2 and the findings from Chapter 3, Chapter 4 presents a theory-driven design study targeted at motivating users to engage with privacy-related information. In particular, we aim to address the limitations of current solutions that primarily focus on improving the presentation of the privacy policy, leaving the motivational issue of privacy unaddressed. The study evaluates the impacts of an enhanced design of the App Store product page on users’ motivation to attend to information privacy. Finally, Chapter 5 concludes the thesis by providing an overview of our work and discussing some limitations of the work and opportunities for future research.

CHAPTER 2 LITERATURE REVIEW

Our work is directly built on existing literature on how end users perceive privacy and efforts to facilitate users' understanding of their online information privacy (discussed in Section 2.1). In addition, we focused on literature around the design for privacy policies to gain an extended understanding of the challenges users face when reviewing privacy policies and the existing work on creating tools and methods to address those challenges (Sections 2.2 and 2.3). Privacy policy is the fundamental, and currently most extensively investigated, informational interface between users and the companies' privacy practices. Including this topic in our literature review provides a feasible scope to establish practically valuable knowledge about how such an interface can be designed. Moreover, while previous literature discussed solutions to simplify privacy policy representation, the end user experience in such solutions depends largely on how developers approach these solutions and consider privacy in the development lifecycle. Since developers are a major force in shaping how technology is built, how they perceive and practice privacy is of great importance to the overall landscape of online privacy. We thus benefit from a review of how developers approach privacy (presented in Section 2.4).

2.1 Investigating Users' Privacy Attitude

Different works have investigated end users' opinions, concerns, and behaviors regarding their online information privacy in various contexts. For example, through a survey study, Gross and Rosson [22] concluded that users express greater concern towards privacy and security than general computer concerns. Various works have also examined users' attitudes and concerns towards their privacy while using different applications and how they perform the delicate risk-benefit analysis when interacting with the app's features. Through examining 5,527 security and privacy-relevant reviews from the top 2,583 apps in Google Play, Nguyen et al. [23] identified that users' primary privacy concerns included storage, contact, and location permissions. On the other hand, Debatin et al. [24] identified that while many Facebook users were aware of and used privacy settings in the application to some extent, they perceived that the benefits of online social networking dominated the risks. Similarly, Xu et al. [25] found that users value personalization over privacy in the context of Location Aware Marketing, a form of targeted advertising that delivers location-relevant ads.

Previous studies also examined issues raised by users on online forums. For example, the study of Li et al. [26] revealed nine primary areas of privacy concerns from 129,075 privacy-related posts in 66 popular software applications and privacy subreddits, with concerns about

“privacy issues and recommendations” and “privacy policies and permissions” being the most popular. They also observed that privacy narratives (i.e., popular and widespread opinions or recommendations) influence user perceptions about software systems and can be linked to users transitioning from one software to another. Similarly, using the `/r/homeautomation` subreddit as a source, Li et al. [27] observed that users’ privacy and security attitudes evolve along the course of their adoption of smart home technologies based on various considerations and contextual factors, such as their technical expertise, preconceptions and assumptions about risks, among others.

Our work complements previous works by investigating a broader scope of users’ general privacy concerns, rather than focusing on a specific domain or technology. Such an approach is useful to understand the multifaceted nature of users’ privacy concerns. We use these insights to provide suggestions for supporting users in the tedious task of privacy management and to redesign the interface for privacy communication.

2.2 Users’ Challenges Concerning Privacy Policy

Previous work has established various challenges that users face when interacting with privacy policies, which can be classified into two broader groups: (1) those concerning the privacy policy itself, and (2) those concerning user perception.

With regard to the privacy policy, users found problems with *the length of privacy policies* [7, 9–12]. For example, Reinhardt et al. [9] attributed the user experience issues of privacy policies to their length. Kelley et al. [10] cited a study estimating an annual loss of productivity amounting to approximately 365 billion dollars if consumers were persuaded to read all the privacy policies they encounter. Quantifying this effort, Adhikari and Dewri [11] mentioned that it would require at least 181 hours per year for a user to read the privacy policies of all used services. In addition, users commented on the *ambiguity, vagueness and lack of transparency associated with privacy policies* [13–16]. In particular, Brunotte et al. [14] acknowledged that the information regarding data practices is concealed within lengthy, unclear, and ambiguous policies. Jesus and Pandit [16] discussed how services seek consent from users through the click of an “Agree” button but later neglect to offer the user additional information on personal data usage or sharing. Ibdah et al. [13] described how participants exhibit distrust towards companies handling their data because of a lack of transparency in the policies regarding the process and evasive practices. The *complex language and legal jargon* employed in privacy policies was another point of concern for users [9, 15, 17]. For instance, Reinhardt et al. [9] found that privacy policies often appear too complex due to their technical language, leading users to conclude that they are not worth the reading ef-

fort. Kelley et al. [10] also discussed that the readability level of typical privacy policies is equivalent to a college education. They noted that company lawyers, rather than customers, often test these policies, explaining the inclusion of complex legal language. Finally, users faced problems with the *evolving and repetitive nature of privacy policies* [11, 18]. Adhikari and Dewri [11] highlighted the difficulty users face in keeping abreast with frequent revisions to privacy policies. Bigrigg and Bigrigg [18] also pointed out that all privacy policies seem identical, and mindlessly reading through them cannot contribute to understanding them.

On the other hand, we also identified problems with users' perceptions of the privacy policy. Firstly, users often felt a *sense of powerlessness* when interacting with privacy policies and protecting their data privacy. In their study, Ibdah et al. [13] discovered that the participants believed the opt-out options to be illusory and designed in a way that does not really allow users to opt out of the service completely. Users in the exploratory design study conducted by Pierce et al. [28] expressed similar frustration over how unreachable or hidden the opt-out options were. Furthermore, users had problems with the *reasoning effort and benefit* associated with reading privacy policies, facing difficulties in assessing the benefit of attending to privacy to warrant the usually significant effort to protect their privacy. Ibdah et al. [13] found that users are often unmotivated to read privacy policies because they do not want to devote the effort and/or just want to receive the benefits of using the service. Kelley et al. [10] also pointed out that users often found it challenging to relate contents presented in privacy policies to their own use of the service.

Understanding the two facets of user challenges concerning privacy policy enables us to get a clearer understanding of users' needs with regard to privacy communication. While taking into account the challenges associated with privacy policy presentation, our work focuses on addressing the problems centered around users' perceptions of the policy to tackle the underlying motivational issue of users' privacy attitudes.

2.3 Design Solutions to Enhance Privacy Policies

To address the user challenges concerning privacy policy discussed in Section 2.2, the literature proposed various design enhancements for the usability of privacy policies. These ideas were either implemented and evaluated by the authors of the reviewed papers or suggested in the papers.

One of the proposed solutions was to *highlight and emphasize the most relevant information* [13, 18, 28–32]. To illustrate, in the study of Ibdah et al. [13], participants suggested that important information in privacy policies should be represented in bullet points and

have a larger font to make it easier to understand. Pierce et al. [28] created printed booklets of privacy policies using graphic design concepts like pull quotes to highlight important points in the policy and observed that they were effective in engaging the users. Wilson et al. [30, 31] developed a tool to help crowd workers annotate privacy policies online, using a machine learning and natural language processing technique to highlight the most relevant paragraphs in the privacy policy for each annotation question. A similar idea has been explored by Tomuro et al. [29]. Bigrigg and Bigrigg [18] developed a JavaScript-based content analysis tool in which the most frequent words in the policy text are identified. Furthermore, two works explored the solution of *notifying users of updates to policies* [11, 16]. Adhikari and Dewri [11] developed a tool that uses natural language processing to highlight key categories of sentences and changes between two versions of a policy. Jesus and Pandit [16] proposed “Consent Receipts” to provide evidence of user consent given for personal data usage. Their tool could alert users of changes to the policy, requiring them to re-consent and regenerate a receipt to acknowledge the changes.

Other studies proposed different forms of *visual aid* to represent or supplement the information in the privacy policy [9, 10, 14, 15, 17]. The study of Kelley et al. [10] represents one of the first attempts at a privacy “nutrition” label, through their design of Simplified Grid. They employed a combination of symbols and colors to represent privacy-related information. Reinhardt et al. [9] explored different privacy policy representation formats aimed at enhancing their usability in a user study, including nutrition labels. Based on the results from the user study, the authors then developed the Visual Interactive Privacy Policy (VIPP) that added interactive elements to the nutrition labels including help icons, expandable rows, and clickable cells for additional information. Brunotte et al. [14] created a tool called Online Privacy Policy eXplainer (PriX) that provides visual interpretations of privacy policies using privacy-related icons. Ghazinour and Albalawi [17] conducted a usability study on the Privacy Policy Visualization Model (PPVM), designed to enhance the representation of privacy policy statements by using visual elements, symbols, and context. Becker et al. [15] included visualizations in privacy policies and investigated their effects on users’ trust towards internet service providers.

Additionally, Ibdah et al. [13] suggested embedding privacy policies directly into mobile apps to *improve navigation* and the overall user experience; the participants in their study found it convenient to have a sidebar delineating the various sections of the privacy policy along with a summary of the policy in each section. In another study, Anikeev et al. [7] developed a 6-point language-independent *readability metric*, called the Global Readability Scale, using popular metrics for English and German texts. They applied this metric to compare the readability of privacy policies from 325 mobile apps in the pre and post-GDPR periods.

While our work draws inspiration from these design solutions, we adopt a theory-driven design approach to systematically guide our design process. In particular, by using components of the Protection Motivation Theory to inform our design ideas, we aim to address the limitations of current solutions discussed in this section that mainly focus on improving the presentation of the policy and providing shortcuts to simplify users’ understanding of the policy. In order to render these current efforts effective, it is essential to address the underlying aspect of user motivation.

2.4 Understanding How Developers Approach Privacy

Online developer forums serve as a community of practice (CoP) for developers to exchange programming-related knowledge and advice with each other. Previous works have explored privacy-related discussions in mainly two popular online developer forums: Stack Overflow [33] and Reddit [34]. Tahaei et al. [33] examined 1,733 privacy-related discussions on Stack Overflow, mainly observing that large tech platforms like Apple and Google play a key role in shaping the definition of “sensitive” information by laying out requirements for communicating privacy information to users through privacy policies and privacy labels. In a related study, Tahaei et al. [35] extracted privacy-related advice present in 119 accepted answers in Stack Overflow to find that many align with Hoepman’s **inform**, **hide**, **control**, and **minimize** strategies, focusing on regulatory adherence and information confidentiality [36]. Li et al. [34] observed that Android developers on the subreddit `/r/androiddev` often show passive attitudes towards privacy, rarely discussing privacy issues concerning personal data, and therefore, advocated for increased transparency and incentives for better privacy practices. Replying on analyzing the distribution of privacy-related keywords, Parsons et al. [37] found that discussions in the `/r/iOSprogramming`, `/r/webdev`, and `/r/androiddev` subreddits mainly focus on app permissions and GDPR compliance, with mostly neutral to positive sentiments exhibited by developers towards privacy issues.

Through directly interviewing developers, some previous works aimed to understand developers’ privacy practices, in particular their challenges. For example, Hadar et al. [38] interviewed 27 developers who performed software design and identified factors influencing developers’ privacy decision-making. They classified those factors into cognitive, organizational, and behavioral, based on Social Cognitive Theory. Their finding indicates that developers experience significant obstacles toward better privacy practice — on the one hand, they have an incomplete understanding of privacy; on the other hand, they have limited options due to the organizations’ privacy policy acting as a powerful force directing developers’ privacy practices. Privacy advocates within an organization can help shift the organizational pri-

vacy culture. Tahaei et al. [39] interviewed 12 privacy advocates within the software team and suggested that despite their enthusiasm, they faced many barriers to implementing privacy. Their effort to promote privacy needs to be supported by the management team and a critical mass of other developers. Tahaei et al. [40]’s work also pointed out developers’ challenges when designing mobile app permissions. Their interview with 19 app developers suggested that while developers made an effort to request permission only when necessary, they faced challenges in understanding the scope of some permissions and were constrained by the third-party libraries’ permission requests. Their findings on developers’ perspective were compared with end users’ perspective, obtained through surveying 309 mobile app users; such a comparison reveals that developers and users are on the same page regarding various aspects related to mobile apps’ privacy, such as the importance of privacy and that users should be ultimately responsible for their privacy choices.

While our work primarily focuses on the end users’ perspective on privacy, comparing our findings with previous work on developers, we can also observe several parallel concerns, which indirectly describe how users perceive the developers’ decisions on design and technology collectively. We make a concrete connection between concerns by different stakeholders and discuss its implications in Section 3.7.3.

CHAPTER 3 ANALYSIS OF USER PRIVACY DISCUSSIONS IN ONLINE FORUMS

The work in this chapter has been submitted to the SIGCHI Conference on Computer-Supported Cooperative Work & Social Computing (CSCW) 2025 and is co-authored by Maggie Xiong, Jinghui Cheng and Jin L. C. Guo. I am the first author of the paper. I have contributed to the conceptualization of the work, the data collection, data analysis and writing of the paper.

3.1 Introduction

This chapter focuses on providing a comprehensive evaluation of users' privacy perspectives and attitudes in order to gain insights that can support users in attending to their information privacy. Online discussion forums provide a platform for users to share their perspectives, experiences, and advice on a wide range of topics. End-user-facing Q&A platforms, such as Quora, play a significant role in collective sense-making, connecting users who seek information with those who possess them. While previous research has investigated how developers use online forums to ask privacy-related questions and approach privacy during the development lifecycle [33–35, 37], very few studies have explored privacy-related discussions from the users' perspective and the existing work mostly focused on users' privacy concerns for particular products [26] or categories of products (e.g., for smart home [26, 27] and mobile apps [40]).

Our research aims to bridge this gap by providing an overview of users' privacy perspectives and attitudes demonstrated in online discussions. Particularly, we analyzed privacy-related questions and their answers from the popular Q&A platform Quora. Quora has an actively growing user base with 400 million unique monthly visitors in 2023 [41]. Compared to other popular online forums, such as Reddit, Quora is a dedicated platform for experience and knowledge sharing and thus is more appropriate for understanding information acquisition and collective sense-making activities. In contrast to developer-centric Q&A platforms, such as Stack Overflow, Quora caters to a broader audience, offering valuable insights from a general user's perspective. By analyzing a random sample of 313 Quora questions and their answers, retrieved from a set of privacy-related keywords, we focused on understanding (1) the privacy topics that the users raised questions about and covered in their answers, (2) the type of information sought by the users in privacy-related questions, and (3) the characteristics of the answers to the privacy-related questions.

Our results revealed a wide range of privacy topics discussed by Quora users, broadly touched upon in questions and their answers, highlighting the complexity of privacy from the users’ perspective. Among the privacy topics, discussions on *privacy protection strategies*, particularly one-stop solutions such as ready-to-use applications or technologies for privacy protection, as well as discussions on *privacy risks and dangers*, particularly societal issues such as surveillance and information leaking, emerged as the most prevalent. We also found that a majority of questions sought *personal opinions* on all aspects of privacy, and many responses were loaded with *emotions* and *personal stories*, indicating that privacy is a subjective experience and reflection of personal values for technology users. This experience, however, is often embedded with users expressing feelings of being overwhelmed by the complexity of managing personal data and a sense of helplessness in protecting their privacy. Our study highlighted the importance of community building and setting industry exemplars to better support users and allowed us to identify opportunities for developers to integrate users’ privacy perspectives into their development processes.

3.2 Previous Studies of Online Community on Quora

Previous works have used Quora to study a variety of topics, such as the linguistic structure of question answerability [42] and detecting experts through features extracted from online traces [43]. In the context of social computing, Quora offers a rich space to study online communities’ concerns and opinions and how they shape their view on different subjects. For example, Mathew et al. [44] studied the nature and factors that drive anonymous posts on Quora and found that users were more likely to discuss topics such as depression, anxiety, social ties, and personal issues anonymously. Das and Semaan [45] used the Bengali Quora forum to examine how marginalized groups can utilize these platforms for collaborative “decolonization work,” to reconstruct their identities and recover from the effects of colonization.

Our work uses Quora as a source to understand the online privacy considerations of users through an interchange of knowledge and opinions. Compared with other forums such as Reddit, where the online community is further divided by specific topics, Quora serves as a general question-and-answer platform and can be considered an integrated community and a direct parallel to users as of Stack Overflow to developers.

3.3 Methods

3.3.1 Data Collection

We used the *quoras* Python package developed by Das and Semaan [46] to collect discussions on Quora. Leveraging Selenium ¹, an open-source, cross-platform web automation framework, the *quoras* package provides various functions to collect information from Quora, including functions to search Quora posts, topics, or users by keyword. Because websites update their code and structure from time to time [47], we reconfigured the package to align with the current Document Object Model (DOM) structure of Quora to accurately retrieve discussions.

We initially employed a process similar to the previous studies of privacy discussions on Stack Overflow [33,35], searching for the keyword “*privacy*” in the question title or tags. However, we observed that using only the keyword “*privacy*” was too broad and returned numerous discussions unrelated to privacy in the context of technologies or software applications. To obtain more relevant questions, we refined our search query to include seven specific terms related to information privacy of technologies or software systems: “*app privacy*”, “*data privacy*”, “*internet privacy*”, “*mobile privacy*”, “*online privacy*”, “*app confidentiality*”, and “*data confidentiality*”. These terms were created by combining the terms “*privacy*” or “*confidentiality*” with terms related to privacy-sensitive technologies found in our initial exploration. Based on these keywords, 1,645 questions were retrieved from Quora as of May 2022. To make it feasible for an in-depth qualitative data analysis, we randomly sampled 313 questions from the retrieved dataset as the target of our analysis; this sample size was calculated with a 95% confidence level and a 5% margin of error. Then, full discussions for these questions (i.e., questions and all answers to the questions) were scraped using *quoras*.

3.3.2 Data Analysis

The data analysis started with an exploration of how Quora users discussed information privacy issues. For this, the first and the third authors randomly sampled and examined discussions from the remaining dataset, excluding the target sample of 313 discussions mentioned above, to conduct an exploratory qualitative analysis. Particularly, we followed a bottom-up inductive coding approach, using Atlas.ti² and following previous guidelines [48,49]. The analysis focused on extracting insights from the following three key elements of the discussions to meet our research objectives of understanding: (1) the prominent privacy topics that were touched upon in the discussions and the questions, (2) the type of information

¹<https://www.selenium.dev/>

²<https://atlasti.com/>

that the questions sought, and (3) the recurring elements in the responses. Starting with 30 discussions, we randomly added new discussions to the analysis until data saturation (i.e., no new topics or themes were found). In the end, 65 discussions were coded during this exploratory phase. During this process, the first and third authors frequently met to discuss the identified themes, resolve discrepancies, and revise and refine the codes. After the initial round of coding, an affinity diagramming [50] activity was conducted to group related topics into higher-level themes. A preliminary codebook was created during this process.

After the preliminary codebook was created, we conducted a three-round refinement process using the sample of 313 discussions. In each of the first two rounds, the first and second authors independently coded a common set of 30 discussions; all four authors then convened to discuss their disagreements and improve the codebook, in hour-long meetings. Topics with a high frequency of disagreement were paid special attention to in our discussions. In the final round of refinement, all four authors independently coded a new sample of 60 discussions (30 discussions per author and each discussion coded by two different authors). Following this round, all authors met again to discuss and resolve any remaining disagreements during two meetings, each lasting 1.5 hours. This iterative process of collaborative coding and resolving disagreements helped pinpoint specific groups in the codebook that caused confusion or required clearer definitions. Based on these discussions, the codebook was finalized by reorganizing and merging some topics, as well as clarifying the scope of specific themes.

Finally, the first two authors applied the final codebook to the entire sample dataset (including reapplying any modified codes on the 90 discussions from the refinement rounds). Among the 313 discussions, 38 were considered irrelevant for one of the following reasons: (1) they addressed privacy or security topics in non-software or digital contexts, such as physical privacy and safety procedures, or (2) the questions did not have any responses for us to analyze. Therefore, the following results were based on the remaining 275 discussions.

3.3.3 Limitations

There are a few limitations related to our methods to be acknowledged. First, we used specific keywords to search Quora questions during our data collection process. Although the keywords were carefully selected, we might still have left out certain discussion topics that were relevant to our study. These discussions or topics could have altered our findings. Second, our final analysis was performed on a sample of the dataset. Although the sample size was calculated to represent the population and the sampling was performed randomly, a sampling error could still occur and bias our results. Third, our analysis was influenced by our experiences and positionality. All authors are experienced in HCI and software engineering

and have investigated user privacy in prior projects. Researchers with different backgrounds may approach the analysis differently.

3.4 Results: Privacy Topics

Discussions of privacy on Quora touch on a wide range of topics, mainly concerning (1) privacy-protecting strategies, (2) privacy risks and dangers, (3) privacy in organizations, and (4) privacy laws, rules, and regulations, either initialized by the questions posted by the Quora users or mentioned in the responses with or without explicitly asking for. Below, we discuss the commonly occurring themes in each category. The numbers in parentheses denote the frequency of the themes, with Q representing the number of their occurrences in questions and R representing the number of occurrences in responses. Each quote can be assigned to more than one theme. Fig. 3.1 provides an overview of the distribution of the privacy topics in the questions and responses.

3.4.1 Privacy Protection Strategies ($Q = 118, R = 252$)

This topic includes various strategies, such as methods, actions, and plans, discussed by users to protect their privacy. We identified many recurring types of strategies, which are reported below. Because of the complexity of the discussions, each question or response may be coded with more than one type.

Applications with Private and Secure Features ($Q = 27, R = 85$) Many users sought and suggested more privacy-friendly and secure alternatives to applications they used, i.e. apps developed with security best practices and implementing robust privacy and security measures to protect user data and prevent vulnerabilities. Some questions directly ask for such apps, for example, “*What are some best apps or websites to keep my photos with privacy?*”, “*Which are the apps of daily use that actually value user privacy and data?*” and “*What is the best internet browser for protecting privacy on a phone? Why? Do you use it?*”. In response, users provided recommendations of various apps, for example, when asked about secure messaging apps, a user wrote, “*Telegram is a good choice. It is pretty secure.*”. Secure browsers like Firefox, Brave, and Tor, and privacy-respecting search engines like DuckDuckGo were also often suggested, e.g. “*The best browser in terms of privacy is the Mozilla Firefox with DuckDuckGo set as the default search engine.*” Some users also recommended Apple’s products and operating systems for enhanced security, as seen in the following response: “*Without a doubt, iOS, iPadOS and macOS are the most private and secure operating systems a common ordinary can use.*”

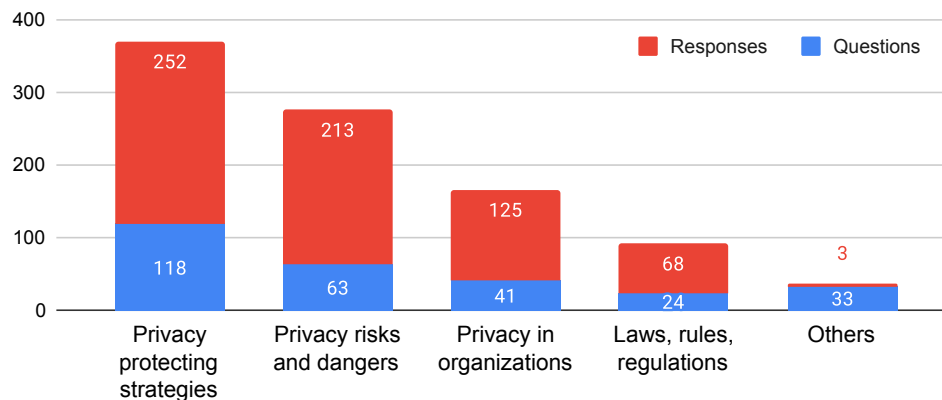


Figure 3.1 Frequency of privacy topics in questions and responses

Applications Built for Privacy and Security ($Q = 22, R = 60$) Several users also asked for or provided recommendations of applications specifically designed to safeguard individuals' privacy and security while using other apps on their devices. Examples of such questions include, “What’s the best ‘secure password app’ to use to secure internet passwords, credit cards, confidential documents, and inheritance?” and “What are the most important internet privacy/security tools for 2019?” Respondents provided a wide range of recommendations, such as browser plugins and extensions, e.g. “Where possible, you also want to install a browser plugin called “Privacy Badger”. It’s also a good idea to install something called “NoScript”. These plugins are easy to get and install in just seconds.”; privacy protection apps, e.g. “Leo Privacy Guard helps to protect the private data information of the user like photos, videos personal contacts and many more.”; and anti-virus tools, e.g. “Kaspersky Mobile Antivirus: AppLock & Web Security - Apps on Google Play I just depend on this app’s anti-theft feature.”, among others.

VPN and Firewall ($Q = 8, R = 71$). Similarly, another common topic found in discussions includes references to VPN and firewall applications to protect an individual’s privacy and personal data. Some questions asked for suggestions of good VPNs, e.g. “What are the best VPN Android apps so far to provide complete privacy?” Others sought more factual information, posing questions such as: “How does a VPN work for online privacy?” and “Do VPNs guarantee internet privacy?”. Several responses highlighted the importance and benefits of VPNs and firewalls in protecting users’ data: “There are scenarios where a protected WiFi could also compromise your privacy, make sure your firewalls and other features are updated and use VPN for more security.” and “A VPN encrypts internet traffic and routes it through servers located in different locations, effectively hiding your IP address and making it difficult for others to track your online activities.”. On the other hand, many users also

pointed out that using a VPN alone is not sufficient to protect an online user’s privacy, as the following statement explains: *“Earlier only using a VPN or a proxy could easily protect yourself from getting tracked online but nowadays it’s just not enough. With a simple proxy or a VPN, it is not possible to prevent browser fingerprinting that can detect even your PC’s operating system. The best way to keep yourself untracked and anonymous while browsing online is by using a multi-login anti-detection browser.”*

Anonymity ($Q = 2, R = 46$). Many respondents recommended providing minimum information to applications and taking measures to stay anonymous online as a means to protect privacy. For example, one user wrote: *“Be cautious when sharing personal information: Don’t give out personal information, such as your full name, address, or phone number, to people or websites that you don’t trust.”* For certain questions posted by developers, some users suggested collecting minimal identifiable information, e.g. *“Don’t use any identifiable user info. We had a product that didn’t use any user info, so we only had their email and proof of payment.”* Two questions asked about solutions that promote anonymity; e.g., *“What are some crazy ideas about what the world needs and should have in terms of online privacy and anonymity to keep companies from spying on us a little too much?”*

Adjusting Settings and Permissions ($Q = 2, R = 44$). Many responses also refer to changing default settings and selectively granting permissions as a way to safeguard their information privacy. As an example, one user suggested: *“You should ensure that you have enabled any privacy settings to limit what other users can see about you and which information the service can collect...”* While providing advice to protect one’s privacy, one user also mentioned that people should *“review every app on your device to make sure that you grant it the minimum permissions it needs to function well, and no more.”* Similarly, two questions inquired about changing an app’s settings, e.g., *“Where can I change the privacy settings in the Facebook Messenger app?”*

Encryption ($Q = 4, R = 39$). Encryption, the process of encoding information or data to make it unreadable, was also a recurring privacy protection strategy mentioned in user questions and responses. Some questions identified were as follows: *“How does the encryption of data impact internet privacy?”*, *“Does the use of encryption ensure online privacy or does it do more harm than good in some cases?”* Several users recommended encryption as a means to secure one’s data, e.g., *“Use messaging apps and email providers that offer end-to-end encryption, such as Signal for messaging and ProtonMail for email. These technologies ensure that only the intended recipients can access the content of your messages.”* Encryption was also often mentioned in conjunction with VPNs. For example, one user wrote that a good way to prevent hacker attacks is *“by using a Virtual Private Network (VPN) which will*

encrypt all network traffic on your device before transmitting them across an open network like the internet. This way everything stays encrypted even after crossing over into an insecure system like the Internet, so no one can get in along the way."

Raising Awareness ($Q = 16, R = 17$). Various user queries sought clarification on the significance of privacy, asking questions like *"Why is internet privacy so crucial in 2020 and beyond?"*. Others aimed to raise awareness about the significance of privacy, as one user posted, *"How can I convince others that online privacy matters and deserves protection?"* Users also asked for resources to expand their own privacy knowledge, for example, *"What are the best internet privacy blogs?"*. Several responses proposed strategies to heighten privacy awareness, for example, reading the privacy policy, *"Although the privacy policies can be long and complex, they will tell you how the companies maintain accuracy, access, security and control of your personal information and how they use your details. Read carefully before you install them, and close the unnecessary permissions of your apps to avoid that they provide your information to third parties."* Some users felt that *"it is [the individual's] responsibility to re-assess all your services and devices which you are connected with to see which data you share to find critical privacy lacks."* *"Training employees to safely process consumer information"* was another proposed strategy. Another respondent highlighted the importance of teaching the younger population about privacy: *"Chat is the best method to keep youngsters safe online. Continue to teach your youngster about the dangers of the Internet..."*

Caution in Online Behavior ($Q = 0, R = 29$). Another common recommendation for protecting individuals' online privacy included being vigilant and exercising caution when using the Internet. Users were informed about several key actions to avoid in order to safeguard their privacy. For example, some responses cautioned about clicking unsolicited links: *"Avoid clicking on links from unfamiliar people and hide postings from accounts"* and advised to *"download apps and files from approved sources. Turn off downloads from unknown sources..."* Other respondents suggested regularly clearing data that can be used to track online activity, for example, cookies or cache: *"Clear your cookies regularly. Most websites may require your cookie to optimize your browsing. However, companies can access your cookies and use your data for targeted ads including location. So remember to clear your cookies regularly especially when you are browsing public websites."* Similarly, some respondents provided directions to hide personal data, as this comment shows: *"To hide your private data, you won't need any special privacy apps. But you will need selected apps like a file explorer, a file opener etc. Most of the utilities required are already provided in almost all latest file explorers like ES file explorer or any your favourite."* Another suggestion was to keep social media accounts private and limit the amount of personal information shared, as a user wrote, *"Try*

not to post personal photos or any pictures of your work, life, families etc. on the Internet”

Authentication ($Q = 1, R = 26$). Several participants emphasized the importance of strong authentication techniques for better security. For instance, to manage passwords effectively, respondents recommended using *“a password manager to create and store complex, unique passwords for each online account.”* Additionally, users highlighted the benefits of screen lock apps and other secure features like facial recognition or fingerprint ID to safeguard their devices, e.g. *“DroidLock Dynamic Lockscreen... secures the device with a very dynamic, ever changing PIN that virtually no one else except you will ever know and “use fingerprinter/Palm Vein Scanner/Face Recognition.”* Users also encouraged the use of additional forms of authentication, like two-factor authentication, because it *“adds an extra layer of security by requiring a second form of verification, such as a unique code sent to your phone and your password.”* One user asked for suggestions for an app to manage authentication: *“What’s the best ‘secure password app’ to use to secure internet passwords, credit cards, confidential documents, and inheritance?”*

Software Updates ($Q = 0, R = 9$). Regularly updating software was one more strategy to maintain privacy, as updates often contain security patches. This is reflected in responses such as *“Update your OS and apps regularly. Developers add improved security features and remove bugs so keep an eye out for updates.”* and *“Always keep your devices updated! Don’t ignore those security fixes and app and operating system updates, they really do matter. Updates are generally free.”*

General Protection Strategies ($Q = 28, R = 0$). Many users posted general questions related to safeguarding one’s privacy. Examples include *“Which layman type practices/ techniques are helping you to secure your Internet Privacy?”*, *“What are the best ways to protect my users’ privacy (websites and apps) in 2020?”* and *“What companies or institutions are available to help me with my online privacy management?”* Some users also expressed concerns regarding protecting their privacy against specific apps, including Quora, for example, *“Today, I ordered checks online for a business I run. Now, two hours later, Quora is running an ad in my feed for check printing. How is this done? How can I better protect my online privacy?”* and *“How much data is being captured by search engines like Google, and how should users protect their online privacy?”*

Others ($Q = 9, R = 8$). In addition to the themes discussed above, a few other infrequent topics emerged from our analysis. For example, some questions were related to protecting the privacy of children: *“What should we do about online privacy protection for children too young to protect themselves?”* Another user inquired about using *“the app privacy report on iOS 15.2”*. One user asked about how individuals in higher positions protect their privacy

and security: *“How do CEOs and Ops staff getting IT systems support for their laptops and mobiles and keeping all their data confidential? What IT security tools do they use?”* In the responses, two users appreciated Apple’s secure hardware, as one of them wrote, *“T2 Security Chip-enabled Macs become nothing more than a brick until the proper credentials are verified, to unlock it Apple led the industry to require that Safari only accept digital certificates that are not more than 13 months old.”* Some users also suggested more primitive methods to transfer data, *“for example by paper mail, which is more difficult to conduct automatic surveillance on”*, or over the telephone, as one user explained that they *“now do as much financial work and banking as I can over the telephone.”*

3.4.2 Privacy Risks and Dangers ($Q = 63, R = 213$)

This topic encompasses discussions of potential privacy-related risks or dangers that could result from their privacy attitude or using an application or software. We identified the following prominent types of privacy risks and dangers mentioned by users. Again, one question or response may be coded with multiple types.

Tracking and Surveillance ($Q = 13, R = 83$). Tracking, collecting, and monitoring individuals’ online activities, behaviors, or location data without their explicit consent, often used for targeted advertising or profiling purposes, was one common privacy risk mentioned in responses, as evident in responses such as *“Today we live in a world where everything is monitored online.”* and *“Likewise with virtually all other apps you use, even the seemingly innocent ones like some ‘flashlight’ apps, which are free because they are actually scraping data from your device.”* Many respondents also expressed concerns about the extensive tracking carried out by large companies, for example, *“If you use Google’s Chrome browser, a myriad of information is sent back to Google, including a browser fingerprint, your browsing history, detailed geo-location information and details about your device. This information is used to establish your identity on any site that uses Google Analytics (about half the internet, as mentioned above).”* Users also occasionally posted questions about addressing the problem of surveillance, as one user asked, *“What are some crazy ideas about what the world needs and should have in terms of online privacy and anonymity to keep companies from spying on us a little too much?”*

Information Leaking or Hacking ($Q = 4, R = 75$). Many responses mentioned the dangers of one’s personal information being exposed and falling into the wrong hands, where it could be misused by hackers or other malicious parties. For example, when answering a question about why privacy on the web is important, a user wrote: *“Hacking has increased a lot in the past few years. With tech giants knowing everything about their users, it is a*

high-security concern among online browsers.” Users also voiced concerns about malware and viruses that could compromise user privacy by stealing personal information or gaining unauthorized access to their devices, as a user expressed: *“Mobile malware has advanced to a new level of sophistication as smart devices continue to gain ground. The number of unique mobile threats grew by 261% in just two quarters. Increasingly complex malware is taking advantage of a wider range of mobile functionalities to exploit vulnerabilities on the device and in the network.”* Some questions also sought advice on what to do in the event of an information breach, e.g., *“I found out a confidential data breach in some random company. ... What should have I done?”*

Sale and Misuse of Data ($Q = 4, R = 57$). On a similar note, responses also mentioned the practice of companies or organizations selling or sharing individuals’ personal information without their explicit consent or knowledge, often for marketing or other commercial purposes. For example, one user mentioned: *“...social media is the biggest source of collecting our personal information... They store it on their servers and then sell it to marketers thus, no privacy is provided. I truly think it’s a violation of our human rights...”* Another user warned about paying more attention to the terms and conditions, *“You know when you just click accept and quickly move on to the next screen. You just GAVE them the permission to sell your info. They do not HIDE anything, everyone knows Data is more valuable than Oil right now! Please think twice before you click ACCEPT...”* An example of a question on this topic is *“When you use a mobile to open garage doors, does the garage door company monitor your activities and invade your privacy, or at least they can sell your activity data to others if they want?”* Similarly, some responses discussed practices of individuals or entities using an individual’s personal data to harass, threaten, or target an individual, e.g. *“You know that I can screengrab that photo in a split second. And then your private photo to a friend is now a digital file that can be shared, copied, turned into memes, and even used in deepfakes to create videos that look like you.”* and *“With issues like social media, big data, cyberbullying and identity theft taking center stage on the news and in lives of people of all ages, internet privacy tools and tactics are in high demand.”*

Third-Party Data Sharing ($Q = 5, R = 54$). Many responses also expressed concerns over the common practice of granting third-party entities access to personal data, which may pose privacy risks if the third party does not implement adequate data protection measures. For example, a user wrote *“When some third party has information about you, it grants them power over your action.”* Again, many users underscored that this practice is common in larger companies and organizations, as these comments show: *“What’s alarming is that social media platforms like Facebook, Instagram and WhatsApp that have access to your personal details can share it with marketers and third party companies.”* and *“If you have an Amazon*

account, Alexa or Prime, they already got all your data. As to sharing it, if you have started to get tons of targeted ads you data was already shared.” Two questions asked users’ opinions about having their personal data shared, *“Are you concerned about Amazon Sidewalk sharing user information? What implications does this have for online privacy and security?”*

Ignorance About Privacy ($Q = 5, R = 23$). Meanwhile, some questions highlighted how many users are ignorant about or disinterested in their privacy, making them susceptible to becoming victims of an information privacy breach, such as *“What do you usually tell people who say that online privacy is not an issue?”* Similarly, this topic was discussed in responses to these questions and others, e.g. *“They know that your phone carries with it a LOT of personal information from banking to email to photos, etc. They also know that most people have no idea of how to do information security well or what info security is.”*

Privacy Concerns in Specific Technologies and Apps ($Q = 21, R = 2$) Several questions inquired about the privacy implications of certain specific technologies, such as artificial intelligence and machine learning, augmented and virtual reality, e.g. *“How is AI and machine learning affecting internet privacy?”* and *“What challenges does AR/VR present in terms of privacy and user experience on mobile platforms?”* Users also expressed privacy concerns for specific products, e.g., *“What are the privacy concerns for TikTok app?”* and *“Should we be worried about internet privacy on Quora?”*

Identification and Deanonimization ($Q = 0, R = 22$). Another privacy risk mentioned was the possibility of associating anonymous or pseudonymous data with individuals’ real identities through different techniques or processes. For example, one user wrote: *“Reddit might not know who you are but people are following you there. And in time, patterns emerge such that people have figured out who is behind those anonymous profiles.”*

Unwarranted Permissions ($Q = 0, R = 12$). Other responses referred to applications requesting excessive or unnecessary permissions, granting them access to sensitive data or device functionalities beyond what is required for their intended purpose, potentially compromising user privacy. For example, one user gave the following advice to protect one’s privacy: *“If you feel the app is asking location unnecessarily, you should deny permission”*

Lack of Privacy on Internet ($Q = 0, R = 7$) Some comments also posited that the internet is an open space where privacy is difficult to maintain, as one user wrote *“The sound, reasonable, and pragmatic approach everyone should take to the internet is that you are in public... That’s the answer, based on working on it and in it for more than 25 years. The internet is NOT private. Period.”* Users also spoke about the permanency of data posted to the internet, even when deleted, for example, *“You can’t delete something from the internet: Whatever you post online, it is there forever. So think carefully before you post*

anything - images, comments, or even likes.”

General Privacy Concerns ($Q = 9, R = 0$) On some occasions, users asked generic and broad questions related to privacy concerns. This includes questions such as “*What is the biggest single threat to internet privacy in the 2020s and why?*” and “*How to fix Internet privacy issues? Why is data privacy an issue?*” Some questions were also related to individuals’ privacy concerns in personal matters, for example, “*Why should I be worried about internet privacy if I only have a small amount of money online?*”

Political Risks ($Q = 5, R = 0$) Some users additionally asked privacy-related questions related to political subjects, such as “*Should internet privacy be an issue for upcoming elections?*” and “*Is sacrificing your online privacy a price worth paying for Brexit?*”

3.4.3 Privacy in Organizations ($Q = 41, R = 125$)

This topic covers discussions concerning how organizations or companies deal with privacy and the privacy aspect of their services. We identified two main themes in this topic.

Company’s Privacy Attitudes and Data Handling Practices ($Q = 31, R = 105$). Many users discussed the attitudes and practices adopted by a company concerning their users’ privacy, touching on how companies collect, store, and process user data. These discussions may focus on ways to promote or violate users’ privacy. In particular, the data practices of large companies drew a lot of attention, like Google, Facebook, Amazon, and Apple. As an example of negative perception towards company privacy practice, one user wrote: “*Google is big on selling users’ information. This means if you are using Google Chrome and you share your location to a website say Facebook, not only are you sharing your location with Facebook but you also are sharing it with Google.*” On the other hand, some respondents appreciated the stance of certain companies on their users’ privacy, for example, “*Apple has identified a market niche they can occupy. They’re the ones that care about you and your data. And since Apple doesn’t make money via advertising, they can afford to care about your data and your privacy.*”

Privacy Policies and Terms of Service ($Q = 10, R = 25$). Some discussions touched on users’ perceptions or the use of the privacy policy or terms of service of a certain company or application. One subject discussed involved drafting a privacy policy for a business, as well as the content and nature of the policy, reflected in questions such as “*Where do I get privacy policy for my iOS app?*” and “*How can it be explained to users for privacy policy that the app read and retrieve contacts?*” Respondents provided detailed explanations, for example, “*There are many places that you can get a Privacy Policy for your iOS app:*

lawyers, generators, or drafting it yourself! Hiring a lawyer is the safest and most reliable option, while drafting it yourself leaves you open to the most risk. Using a generator is a ‘happy medium’ that can provide a suitable Privacy Policy for most iOS apps...” Additionally, users asked questions about the privacy policies of apps and services they used, for example, *“What popular apps or websites have a privacy policy that should concern me and might affect the degree to which I use those sites or apps?”* Similarly, respondents expressed their attitude towards privacy policy as seen in this comment: *“Nobody reads privacy policies before joining a platform like Facebook or Google. They constitute thousands of words of legalese, a construction that literally requires a law degree to parse and begin to understand.”*

3.4.4 Privacy Laws, Rules and Regulations ($Q = 24, R = 68$)

This topic includes discussions related to different privacy laws and regulations and their compliance. Two themes were identified.

Requirements Specified by Regulatory Authorities ($Q = 21, R = 63$). Various discussions referred to privacy-related laws and regulations established by authoritative entities, as well as the compliance of organizations and applications with these laws and regulations. Some users asked about the implications of implementing certain laws, e.g., *“How will the US Congress and Trump’s rollback of the FCC’s Internet privacy protections affect Internet privacy for users of ISPs in other countries?”* and *“Is internet privacy no more in India after the new law for VPN providers?”* Others raised questions about the differences in laws and regulations across regions, such as, *“Why does the European Union have strict internet privacy laws?”* and *“How does the US’s internet privacy compare to that of other countries?”* This aspect was mentioned in responses to other questions as well, for example, when a user asked if complete internet privacy will ever exist, one response highlighted: *“In the EU, they have extensive privacy laws regarding consumer data — they treat it like consumer protection — including the ‘Right to be Forgotten,’ where you can request that all the data associated with your account be destroyed.”* Users also discussed the legal requirements for privacy policies: *“The main risks are that privacy laws can be quite specific, and in some places very comprehensive. If you miss something out, your Privacy Policy may not be suitable at all, and may leave you open to fines or regulatory action.”* Often, specific laws or regulations were also mentioned, as seen in comments such as *“The Federal Trade Commission enforces laws such as the Children’s Online Privacy Policy Act and the CAN-SPAM act.”* and *“In the EU, the General Data Protection Regulation has created pioneering conditions for individuals to take control over their online data and empower themselves.”*

Requirements Specified by App Store Platforms ($Q = 4, R = 7$). Occasionally, users

also talked about requirements imposed by App Store platforms like Google and Apple on their developers or users. For instance, one response stated about privacy policies of Android apps: *“It’s also important to disclose specific information being collected from your user i.e: login, camera, contacts, etc. Since February 2017 Google enforces a strict privacy policy requirement on apps requesting sensitive permissions and user data.”* Similarly, another answer mentioned that *“Google requires users of Google Analytics to use a privacy policy. When you sign up for Google Analytics, you consent to their terms that state under, you ‘(...) will have and abide by an appropriate Privacy Policy (...)’”* Users also clarified doubts they had regarding the requirements, for example, *“Do you have to reveal your use of third party API’s, and their own collection of user data, in your app’s privacy policy?”* and *“Does the Apple app store require you to have a terms of use and privacy policy for your iOS app?”*

3.4.5 Other Topics ($Q = 33, R = 3$)

Some questions and a few responses touched on topics that did not fall into the categories discussed in the previous sections. For example, some questions were of an abstract or philosophical nature. Such questions include: *“When is internet privacy necessary?”*, *“Is internet privacy a human right?”*, *“How to feel about internet privacy?”* and *“What is the maximum level of online privacy right now?”*

A few users posted questions related to the difference between privacy and security, for example, *“What is the difference between Privacy and Security with reference to a user’s data on the Internet?”*, to which one user responded that *“privacy is about controlling who can access an individual’s data, while security is about protecting the data from being accessed by unauthorized individuals or entities.”*

Some queries concerned individuals’ attitudes towards their privacy, e.g. *“What sensible reason could someone tell me to give up my internet privacy or any of my freedoms?”* and *“Is getting internet privacy worth spending money on? What do you think?”* Similarly, two responses mentioned this subject. One user wrote, *“Media consumers expect streaming services to offer experiences tailored to their watch history and tastes, but they are also more concerned than ever with what data is stored about them and why.”*

There were additional questions that discussed different topics, such as the dark web, e.g., *“What role does the deep web play now and in the future when concerning internet privacy?”*; and political subjects, e.g., *“What is President Trump’s position on internet privacy?”*

		Response Topics			
		Protecting strat.	Risks/dangers	In organ.	Laws/rules/regs
Question Topics	Privacy protecting strategies	75%	44%	30%	10%
	Privacy risks and dangers	43%	76%	40%	17%
	Privacy in organizations	37%	54%	56%	22%
	Laws, rules, regulations	25%	46%	50%	96%

Figure 3.2 Percentages of questions in each privacy topic answered with responses touching on each topic

3.4.6 Relationship Between Question Topics and Response Topics

To understand how the topics in questions were answered, we analyzed the distribution of privacy topics that appeared in the responses among those raised in the corresponding questions (see Fig. 3.2). The percentages were calculated as a ratio of the total number of times a privacy topic appeared in the responses for a corresponding privacy topic in the question against the total number of occurrences of that privacy topic in the questions. As expected, privacy topics asked in the questions were most frequently responded to with answers covering the same topics. Interestingly, in questions concerning the topic of privacy in organizations, responses discussed privacy risks and dangers (54%) almost as frequently as the topic itself (56%). Privacy laws, rules, and regulations remained the least discussed topic when responding to all question themes except when it was the primary topic asked, in which case, it is almost always mentioned again in the response. Additionally, a noteworthy correlation emerged between privacy risks and dangers and privacy-protecting strategies; each topic appeared as the second most prevalent topic in responses to questions centered on the other topic.

3.5 Results: Types of Questions

We identified three categories of information that Quora users sought when posing questions, i.e., opinions, facts, and instructions or guidance.

3.5.1 Opinion ($N = 135$)

These questions sought the respondent’s opinion or perspective on a privacy-related topic or issue, generally inviting subjective responses. Answering these questions often requires some interpretation and assessment by the respondent based on some evidence. Some questions asked for users’ personal or technical opinions on general privacy-related topics, such as “*Do you allow your children to use Facebook’s Messenger Kids application given its recent privacy issues?*” and “*Is the best way to protect your privacy on Facebook to not use any applications?*”. Other questions were concerned with respondents’ interpretation of the intent behind a specific action, policy, or decision of another party or the behavior of individuals in general. Some examples include “*Why will Google like Apple also implement the nutrition label privacy labels on all Android applications distributed on the Play Store?*” and “*With all the talk about online privacy, why do people still choose to put smart devices in their home when companies like Amazon have admitted to listening in to private conversations?*”. In addition, some users sought to understand the potential privacy-related consequences or impacts of a specific action, policy, decision, or technology. For example, one user wrote: “*How will stricter internet privacy regulations impact a typical user?*” Another user expressed their concerns about COVID-19 contact tracing apps: “*What are the privacy implications of Google and Apple Covid-19 virus contact tracing apps?*”

3.5.2 Factual ($N = 104$)

These questions sought factual, objective information about a privacy-related topic or issue. While factual information also requires a certain degree of interpretation, they often have definitive answers, unlike opinion questions, which typically lack a clear right or wrong answer. Some questions in this category asked for technical details about privacy-related problems, such as “*Which web application attack is more likely to extract privacy data elements out of a database?*” and “*Can another application or browser use our privacy and data on a large scale with the help of Chrome?*” Some other questions sought information about privacy laws, regulations or organizational rules, such as “*Does the Apple app store require you to have a terms of use and privacy policy for your iOS app?*” and “*How long before “the right to be forgotten” (internet privacy) becomes law in the United States?*”. Moreover, users also posed questions to gain factual information about certain applications or technologies, such as “*What are some of the privacy features on the Signal app?*” and “*Is the cloud a safe environment to store confidential data?*”

		Question Types		
		Opinion	Factual	Guidance
Question Topics	Privacy protecting strategies	39%	25%	47%
	Privacy risks and dangers	60%	38%	6%
	Privacy in organizations	49%	44%	15%
	Laws, rules, regulations	46%	88%	0%

Figure 3.3 Percentages of questions in each privacy topic that were asked with each question type

3.5.3 Instruction or Guidance ($N = 66$)

These questions specifically looked for information or guidance on performing a particular action. The instruction provided can be subjective or objective. The responses to these questions generally provide a basis for action for the questioner. For example, “*How do I maintain privacy of user data in SAAS application?*” and “*Where can I get some templates/drafts of terms of services and privacy policies for my web application?*” Some users also asked for suggestions of tools that can help users protect their privacy, such as “*What are the applications one should install before going online to ensure privacy and protection?*” and “*What is the best internet browser for protecting privacy on a phone? Why? Do you use it?*”

3.5.4 Relationship Between Question Types and Question Topics

We analyzed the proportion of the three question types for each privacy topic covered in the questions to understand the aspects that the users were interested in for each topic (see Fig. 3.3). The percentages were calculated as a ratio of the total number of times a question type appeared with a particular privacy topic in the question against the total number of occurrences of that privacy topic in the questions. For questions about privacy risks and dangers and privacy within organizations, users most frequently searched for others’ opinions (60% and 49% respectively). Meanwhile, suggestions or guidance were least sought for all topics except questions on privacy protection strategies (47%). Further, most of the questions about privacy laws and regulations were factual questions (88%), with about half asking for opinions (46%) and no inquiries requesting guidance on legal matters.

3.6 Results: Characteristics of Responses

To understand how the community reacts to the privacy questions, we characterize the responses based on their style, nature or format. We observe that the responses are rich in strong sentiment, concrete and illustrative examples, external resources, and personal stories.

3.6.1 Emotional Arousal ($N = 147$)

Users sometimes expressed strong emotions in their responses that hinted at their perception and attitude toward the subject being discussed. Some users conveyed **contempt** towards certain matters or to the questioner, as seen in this statement: *“Hello naive stranger! Companies do not SELL data to the government in China. Companies provide data access to law enforcement when requested. There is no money involved.”* **Sarcasm** was a tactic sometimes employed when responding to questions that the respondent viewed as seemingly trivial; e.g., *“I have a very simple test for how important online privacy should be to you: Please post your full name, address, phone number, social security number, bank account numbers, and credit cards. Post the names, ages, and schools attended by your children (this is of course after posting your bank account information). Please put up an active webcam in your bathroom pointing at your toilet. Once you have done all of the above, let’s continue this discussion about online privacy.”*

Occasionally, users also indicated a sense of **helplessness** towards their privacy in responses such as this one: *“But reflect, what are they going to do with this information? You really cannot do much about that either. So why worry about this, all you will do is put more worry in your head?”* Similarly, some users added depth to their answers by including **thought-provoking questions** that encourage readers to reflect on the topic.; e.g. *“When someone hacks and steals data from any platform, be it FB, google, yahoo, a bitcoin exchange, who can say confidently that their information has not been harvested, and by extension, that they have been compromised? In this, the twenty first century, can we do without all the online services? ...Can we accept that if and when we use these services, we tend to loose our identity a little at a time? I think, a resounding yes. Is it possible that every netizen, (internet user) has somewhere, somehow been compromised, and we are totally unaware of it? I think, yes. Solutions, any one?”* In addition, some users expressed **radically different opinions** compared to other responses to the same or similar question. To illustrate, when a user asked about the most secure operating software for phones, one of the responses was, *“In my opinion, online privacy regulation should be mandatory and enforced by draconian punishments. I should be the final arbiter of where my data goes, who can see it, what it can*

be used for.”

3.6.2 Example ($N = 136$)

Providing examples or illustrations to support a point or idea was a common tactic used in responses. For instance, one user provided the following account while explaining the need to care for one’s privacy: *“Earlier this year, a young woman purchased a few nondescript items such as cotton balls, unscented lotion and some vitamins. Based on what the company already knew about her, they were able to correctly predict that she was pregnant, and began targeting her for baby items by sending her coupons in the mail. The issue? She was a teenage girl, and these coupons alerted her father that she was indeed pregnant.”* Another user included a diagram to explain the concept of VPN: *“Here’s a quick drawing to make this more clear, I hope. The traffic between your device and the bank is represented as the pink arrows. It will be protected by the VPN, but only between you and your VPN provider. From your VPN provider to your bank it’s relying on the TLS encryption that’s inherent to HTTPS.”* Many users also employed illustrative comparisons to clarify their point. For example, one user wrote about the risk of having one’s online privacy compromised: *“Anytime you go online you take that risk. Just as you do everytime you get in a car or buy a lottery ticket. The difference though is i still have a choice to get into a car or buy a lottery ticket but my choice to use the internet is being slowly taken from me because for many businesses, agencies, etc.. thats the only way they are now accessed.”*

3.6.3 External Source ($N = 58$)

Some respondents included links to articles, websites, videos, and/or other Quora discussions for readers seeking more information. Some examples include *“Here is a link that will give you more insights on online privacy”* and *“If you want to secure your android mobile data. See this video below, hope it may help you to secure your data.”* These external sources provide further content or support for the discussion question. Sometimes, representative of organizations or companies responded to users’ queries and linked to supplementary information on their websites. For instance, a representative of the mobile network company, T-Mobile, responded to a question regarding its modified privacy policy: *“We may occasionally ask you to confirm your choices. Please see our advertising choices section below for more information.”*

3.6.4 Personal Experience ($N = 56$)

Users also recounted their own experiences, preferences and actions in their responses, either as examples to reinforce their viewpoint or as a source of guidance. For instance, while arguing about the prevalence of Google in our every daily lives, one user wrote: *“Let me tell you an interesting fact, I myself am using Quora on google right now. But that doesn’t mean I’m entirely reliant on Google. I use Firefox often, I use VPN all the time and for my smartphone, I use this app Tor browser private web + vpn. I try to take at least some measures that can reassure that I’m trying to save my privacy.”* Users also often gave recommendations of apps or services that they personally used and tested, e.g., *“I use LastPass . It is great and secure. If you are looking for open-source then KeePass (software) is not bad. Then you have 1Password , Dashlane and others, I tried them but they were not as good as Lastpass.”*

3.6.5 Relationship Between Response Characteristics and Response Topics

To investigate how the answers concerning each topic are phrased, we calculated the frequency of the response characteristics that appeared in the responses for each privacy topic (see Fig. 3.4). Examples were consistently the most abundant component found across all the response topics. Additionally, users frequently expressed emotions in responses touching on privacy laws, rules and regulations (22%) and privacy risks and dangers (21%). Personal experiences were also fairly frequently discussed in topics (more than 10% of the responses) other than privacy laws, rules and regulations. On the other hand, the external source was the least frequently seen characteristic in responses, except for those touching on privacy laws, rules and regulations (13%).

3.7 Discussion

Privacy for users is a multifaceted concept. Our study reveals the intricacy of users’ discussions on privacy, touching considerations across individual, organizational, and societal levels. Their responses to privacy issues are often value-laden. While they frequently share their sense of being powerless in the current technological landscape, they are also collectively showing resistance to the invasive privacy culture by recognizing and adopting privacy-advocating means and technologies. In this section, we contextualize our findings from those aspects and discuss future directions for practitioners and researchers.

		Response Characteristics			
		Emotion	Example	Ext. source	Personal
Response Topics	Privacy protecting strategies	9%	21%	8%	14%
	Privacy risks and dangers	21%	28%	6%	10%
	Privacy in organizations	16%	26%	6%	10%
	Laws, rules, regulations	22%	37%	13%	4%

Figure 3.4 Percentages of responses containing each privacy topic identified with each response characteristic

3.7.1 The Complexity of Privacy Topics

Our analysis of privacy discussions on Quora revealed that users are interested in a wide range of privacy topics, seeking varied types of information, and leveraging different resources to back up their discussions. These characteristics demonstrate a collective sense-making process in which users keep treading water, trying to manage the complexity of privacy together. This complexity is first revealed in the various layers of privacy concerns touched upon in user discussions, from personal to societal. At the **individual layer**, users discussed the problem of *Ignorance About Privacy* and the importance of *Raising Awareness* and practicing *Caution in Online Behavior*. At the **technology layer**, users worried about risks like *Information Leaking or Hacking* and *Identification and Deanonimization*; at the same time, they listed various techniques for protecting privacy, such as *VPN and Firewall*, *Encryption*, and proper *Authentication*. At the **organization and application layer**, users raised concerns towards *Third-Party Data Sharing* and *Sale and Misuse of Data* and questioned *Company's Privacy Attitudes and Data Handling Practices*; they advocated for *Applications with Private and Secure Features* and *Applications Built for Privacy and Security*, preferring apps that allow *Adjusting Settings and Permissions*. Finally, at the **society layer**, users actively sorted understanding of the privacy *Requirements Specified by the Regulatory Authorities*; they highlighted the problem of the ubiquitous *Tracking and Surveillance* and an overall *Lack of Privacy on the Internet*. All four layers collectively affect users' attitudes toward privacy, which eventually influences the users' preferences and behaviors when using various technologies, applications, and platforms.

The complexity of privacy is also evident in the interconnections formed between the topics asked in the questions and those involved in the responses. As our results indicated (see

Figure 3.2), although topics mentioned in the responses frequently echoed those raised in the questions, other topics were often touched upon. Interestingly, answers to questions about privacy in organizations, in particular, in large technology companies, often featured privacy risks and dangers almost as frequently as the main topic itself. Many users were aware of, and critical of, companies’ abusive power over their data. This awareness is evident in questions like *“How much data is being captured by search engines like Google, and how should users protect their online privacy?”* and *“Is the significant loss of online privacy worth joining TikTok?”*. Responses to those questions often revolved around concerns about large-scale data collection and invasive tracking methods employed by large companies for targeted advertising or third-party data sales. On the other hand, however, there were also mentions of organizations or applications viewed positively for their privacy practices; users recommended choosing certain companies as *Privacy protection strategies*. For example, one user wrote, *“Apple has a deep commitment to privacy and designs their products to collect the least amount of information needed, vs the most information possible that Google does.”*

3.7.2 The Overwhelmed and Often Helpless Users

Our results indicated that, from the users’ perspective, privacy is frequently discussed as a subjective experience. A majority of questions sought personal opinions (see Section 3.5), and many responses were loaded with emotions and personal experiences (see Section 3.6). Extreme opinions and strong emotions such as sarcasm and contempt were frequently observed when users discussed various privacy topics, exemplified in statements like *“Why? Because it’s YOUR personal and sensitive thing. If I ask you to give me your personal information, will you give me? It’s hell no, right? But, why do YOU give your personal information away to Google, Facebook, TikTok, Microsoft, Apple, etc. when they ask you? And you willingly and blindly give them. Why? Think about it.”* The prevalence of such emotions implies that privacy goes far beyond technical or abstract concerns but is considered by users a fundamental individual value. Such emotions, however, create an interesting contrast with the vast amount of user comments questioning the feasibility of effectively protecting their privacy. The users’ discussions often implied that they were overwhelmed by the complex task of managing their personal data and voiced a sense of helplessness in protecting their privacy.

Our results also indicate that users tended to mention one-stop solutions (e.g., applications with private features or built for privacy) more often rather than fine-tuned personal effort (e.g., adjusting settings and permissions, practicing caution in online behavior) when discussing *privacy protection strategies*. Some suggestions for personal effort are also quite extreme and ceased to be feasible. This echoes with previous work indicating that users often

are not equipped with sufficient knowledge, are not provided with appropriate options, or do not have the time [51] to manage their privacy, and thus have to adopt readily available solutions. Moreover, our findings about users' perceptions towards industry leaders' privacy practices highlighted a continuing dilemma: these companies often operate on the “economics of personal data” [52] but the current technology landscape also makes it almost impossible to live without them. So, although it is perceived users' “*responsibility*” to protect their privacy, they often do not have the power to actually do so, as a user mocked such a reality: “*Privacy is just a CONCEPT... You need not to worry about it. Just use it, enjoy it and throw it away. Ha ha ha...!!! LOL...!!!*”

As a result, many users expressed a readiness to trade privacy for the convenience offered by the technology, as a user stated this case by saying, “*So I'll start by saying that ‘Privacy has become synonymous to comfort.’ ... We are compromising our privacy more because we want comfort in everything...*” Another user mentions how people will inadvertently provide whatever information is necessary to receive services, “*Yes, Internet privacy is dead. This is self inflicted as people got addicted to free services and provide their information online.*” These comments support previous research indicating a privacy/convenience tradeoff experienced by users [53, 54], as well as aspects of the privacy calculus theory [55], which posits that individuals engage in a cost-benefit analysis when deciding to disclose personal information, weighing the perceived benefits against potential privacy risks. This also aligns with prior research findings that suggest personalized services positively influence consumers' perceived benefits, subsequently affecting the intention to disclose personal information [25, 56, 57]. There is no easy fix to this, as a user mentioned, “*Companies will build in strong privacy only when there's a proven market demand for it. So far, for the most part, people are willing to give up a lot of privacy for convenience.*” The recent work focusing on motivating users to attend to their privacy [58] may offer some insights for addressing this issue.

3.7.3 Comparing Developer and End User Privacy Discussions in Online Forums

Previous studies have extensively investigated developers' perspectives on privacy manifested on online forums [33–35]. Fundamentally, the scope of the privacy-related discussions by the end-users is largely different from those made by the developers. Developers predominantly engage in discussions that revolve around different phases of application development [34], encompassing coding practices and legal considerations pertaining to privacy requirements [33, 35]. These discussions underscore technical intricacies and compliance measures inherent in the development process. Conversely, users participate in privacy dialogues within the context of software application usage and cyber hygiene. Our results indicated

that users’ primary focus is on acquiring knowledge to comprehend various privacy-related concepts and to make more informed decisions regarding the practical use of these applications or technology in general.

Despite the fundamental differences between the perspectives of the two types of stakeholders, we found similar themes in the advice offered by respondents in both contexts. For example, to ensure the confidentiality of their users’ data, developers suggested employing techniques like encryption, hashing and protocols like HTTPS [35]. These same suggestions were also prevalent in the privacy-protecting strategies offered by users in our analysis (presented in Section 3.4.1) Developers predominantly emphasized the incorporation of encryption techniques at a technical level, for safeguarding databases, passwords, and audio/video streams within their applications [35]. We found that users actively advocated for a wide range of complementary privacy-centric tools, endorsing the adoption of applications and technologies inherently equipped with encryption features like encrypted communication apps (e.g., Signal), Virtual Private Networks (VPNs), encrypted email services, and secure browsers, among others. This parallel creates a powerful positive cycle: developers implementing robust privacy-preserving measures attract users seeking secure solutions, while user preferences for such technologies incentivize developers to prioritize privacy in their applications.

Similarly, other elements common to both groups were related to third-party services and verifying permissions and policies. Developers received advice to familiarize themselves with and understand the extra permissions required when integrating third-party services [35]. Meanwhile, we found that users were cautioned to exercise prudence when interacting with applications using third-party services. A related recommendation for developers involved scrutinizing the permissions and policies of ad networks they employed [34, 35], while our results indicated that targeted advertising was a recurrently discussed privacy risk in user conversations. Combining these results, we might conclude that both developers and users are encouraged to actively understand the privacy practices of the services they interact with, whether during the development phase or while using the application. However, developers find themselves in a different position as they possess the technical prowess to address these issues proactively, thereby alleviating the burden on end users. Developers are essentially the “mediator between platforms and end-users” [40]. By prioritizing privacy during development, developers can create a more secure and transparent digital environment, easing the burden on users to navigate complex privacy choices [34], and ultimately help users combat the ongoing battle of managing their privacy [51].

3.7.4 Implications to Practice and Research

Our study provides various implications for future practice and research. First, **supporting communities for privacy-related experience sharing** is important to allow users to collectively navigate through the complex but personal topic of privacy. While Quora and other platforms such as Reddit and Stack Overflow partially serve this purpose, the discussions on relevant topics can be buried by opaque recommendation mechanisms and some recommendations may not be credible. Moreover, explicit recognition of the personal and emotional dimensions of privacy issues can lead to enhanced communication strategies that build trust and encourage proactive behaviors, user-centric privacy solutions, and policies that take users' personal stakes into consideration.

Second, **exemplars (e.g., influencing companies or apps) need to be set towards empowering users to attend to privacy**, increasing transparency about data collection and offering users more control over their data. While Tahaei et al. [33] highlighted the role of large organizations in defining privacy requirements for developers and setting the standards for sensitive information, the user discussions from our study ironically showed that some of these corporations are often critiqued for not meeting their own privacy standards. By aligning the operations more closely with the privacy standards they set, these companies or other influential exemplars can become powerful precedents to encourage a more comprehensive adherence to privacy requirements across the technology landscape.

Third, **streamlining the communication between developers and users about privacy** would help them better understand the users' perspectives and create better privacy solutions. The subjective and non-technical aspect of privacy is rarely discussed in developer-focused forums. By understanding this complexity and developing empathy for user values, developers may be more encouraged to provide useful privacy features to increase user adoption and bridge the gap between users' interests and actions.

3.8 Conclusion

The importance of information privacy is more critical than ever in the current digital landscape, especially for technology users. Through analyzing the discussions about privacy-related topics on Quora, we identified four categories of topics users touched on in their questions and responses. Among them, privacy topics such as privacy-protecting strategies, particularly regarding secure applications, and privacy risks and dangers, including tracking and information leaks or hacking, were most discussed. Meanwhile, our analysis suggests that privacy-related questions frequently seek personal opinions, aside from factual information

and guidance. At the same time, responses to different topics are rich in information, such as examples and external links, and reflect personal experience and values. Overall, our study depicts users' perspectives concerning privacy, illustrating how they navigate the current digital landscape with caution and sometimes with despair. Our work complements previous work on users' and developers' privacy attitudes and suggests directions to move forward, including the importance of experience sharing among users, setting exemplars for privacy best practices, and communication between developers and users about privacy concerns.

CHAPTER 4 THEORY-DRIVEN DESIGN STUDY

The work in this chapter has been published in the proceedings of the ACM Conference on Designing Interactive Systems 2024 and is co-authored by Maggie Xiong, Jinghui Cheng and Jin L. C. Guo [58]. I am the first author of the paper. My contributions include the conceptualization of the work, design ideation, development of the conceptual prototype, user study (online experiment and interviews), data analysis, and writing of the paper.

4.1 Introduction

In this chapter, we focus on addressing the gap between users' privacy concerns and their motivation to actively attend to privacy through a theory-driven design approach [19]. Particularly, we employed the Protection Motivation Theory (PMT) [1,20] to inform design ideas specifically aimed to encourage users to take an interest in attending to their information privacy. We then used those initial design ideas to create a conceptual design prototype, enhancing the current App Store design with five features: (1) a privacy FAQ, (2) a rating on the privacy practices of the app, (3) tutorials on customizable options related to privacy, (4) a prompt for users to review privacy information, and (5) user reviews related to privacy.

To evaluate the potential impact of our conceptual design and the underlying design ideas, we conducted an online experiment followed by a set of interviews, comparing our design with the existing App Store interface. The results showed that our design was successful in motivating users to attend to privacy. The design elements aimed to reinforce users' threat and coping appraisals (i.e., two main factors in PMT, see Section 4.3) made our participants sensitive towards their privacy in the application. In particular, participants appreciated the level of detail and organization of information in the design. They perceived such information as helpful for making better-informed decisions and taking actions regarding their personal data in the application. At the same time, to further enhance user motivation, the information needs to be condensed even more and potentially restructured. Overall, our research contributes to the ongoing effort to streamline privacy communication by targeting the inherent but often overlooked motivational issue related to privacy awareness. Our specific contributions are three-fold. First, we demonstrated a theory-driven design approach based on PMT that led to fundamental design concepts for motivating users to attend to privacy. Second, our approach created concrete design categories and features that can guide design efforts to directly target user motivation issues for privacy. Third, the results of our study provided considerations and practical implications that can inform future design.

4.2 A Narrative Literature Review on the Design for Privacy Policies

We started with a narrative literature review [59,60] on the design for privacy policies to gain an extended understanding of the challenges users face when reviewing privacy policies and the existing effort on creating tools and methods to address those challenges. We focused this literature review on privacy policy because it is the fundamental, and currently most extensively investigated, informational interface between users and the companies' privacy practices. A literature review on this topic provides a feasible scope to establish practically valuable knowledge about how such an interface can be designed. Additionally, we adopted a narrative literature review approach rather than aiming to systematically synthesize all previous work published for informational interfaces for privacy; this approach enabled us to critically reflect on major related work on how to communicate privacy policy in-depth and to focus on opportunities that can be tackled by our study [60]. The detailed findings of the literature review are presented in Sections 2.2 and 2.3; this section explains the steps followed to conduct the narrative literature review.

We conducted our search on two databases: the IEEE Xplore database and the ACM Digital Library. We chose these two databases since they both feature a wide selection of peer-reviewed works that concentrate on the design aspect of computing technology. Together, they provide high coverage of the most cited HCI venues, publishing or indexing most of the top 20 HCI journals or conferences based on h5-index [61].

We first conducted our search using the keyword “privacy policy” in August 2022 to find 1061 papers in total (722 and 339 papers, in IEEE and ACM, respectively) with the publication of the papers ranging from 2007 to 2022. We then filtered the papers using their titles and abstracts following two inclusion criteria: (1) the paper must focus on privacy policies of applications or services, and (2) the paper must include the users' perspective towards privacy policies. Four authors split the task of the initial filtering; they labeled each paper as either “include”, “exclude”, or “maybe,” and noted their reasons for each decision. The four authors then discussed and resolved any uncertainties and disagreements. This initial filtering process resulted in 19 papers to include for detailed review.

Next, we read these 19 papers, focusing on extracting the information from each paper about (1) the challenges users faced when reviewing privacy policies, and (2) the solutions and/or designs proposed to address those challenges. During this review process, three papers [62–64] were further eliminated as their focus was not relevant to our study, resulting in the final list of 16 papers. The four authors then met and conducted an affinity diagramming [50] activity to group the extracted information from the 16 papers into categories to identify common

themes. The results of the literature review, including the specific themes are discussed in Sections 2.2 and 2.3. Table 4.1 summarizes a mapping between the reviewed papers and the themes.

4.2.1 Discussion and Reflection

Through this narrative literature review, we identified six challenges of users when interacting with privacy policies and attending to their information privacy. Four of those challenges were related to the presentation of the privacy policies themselves, while two were associated with users' perceptions of protecting their information privacy in apps and services as a whole. We also identified six design aspects explored in the literature that aimed to support users in interacting with privacy policies. Notably, these design solutions almost exclusively focused on the immediate problem of making the privacy policies easy to understand for users, mostly by improving presentation and providing shortcuts. However, the vital issue related to users' perceptions of the privacy policy, as well as their overall information privacy, is not systematically or effectively addressed in the previous work.

Besides the works reviewed, there are other similar efforts to make information related to the privacy practice of an application or service easy to access and understand, using techniques such as contextual privacy notices [5, 65, 66] or privacy visualizations [67, 68]. For example, Ebert et al. [66] found that salient and concise in-app privacy notices are effective in raising user awareness. Similarly, there are standardization efforts made by Apple's App Store¹ and Google's Play Store² requiring app developers to input privacy summaries and labels describing their application's privacy practices. However, through our preliminary discussions with users of mobile apps and online services, we found that users still do not pay attention to these privacy summaries and labels. Although they agreed with its importance when asked explicitly, they do not necessarily care to take concrete actions to protect their information privacy [69]. While we acknowledge that a user may not need to engage with privacy at all times [51], such engagement becomes important in situations where the sensitivity of personal information is elevated and the stake of compromised privacy is high. Therefore, addressing the underlying motivational issue remains essential to make the existing effort about privacy policy presentation effective, eventually empowering users to protect their information privacy. We thus aim to contribute to this aspect and explore design guidelines and solutions that focus on motivating users to attend to their privacy when using apps and services. Particularly, we adopted a theory-driven approach to orchestrating our design pro-

¹<https://developer.apple.com/app-store/app-privacy-details/>

²<https://support.google.com/googleplay/android-developer/answer/10787469>

Table 4.1 Papers included in the narrative literature review and the extracted challenge and design categories.

	Challenges identified				Proposed design ideas					
	Length	Ambiguity, vagueness	Complexity and jargon	Evolution and repetition	Control autonomy	Effort vs. benefit	Highlighting info.	Notification	Privacy labels	Other visual aid
Kelley et al. [10] (2009)	×		×			×			×	
Becker et al. [15] (2014)		×	×							×
Talib et al. [12] (2014)	×									
Biggrig and Biggrig [18] (2015)				×			×			
Ghazinour and Albalawi [17] (2016)			×		×					×
Tomuro et al. [29] (2016)							×			
Wilson et al. [31] (2016)							×			
Pierce et al. [28] (2018)		×			×		×			
Wilson et al. [30] (2018)							×			
Adhikari and Dewri [11] (2021)	×			×				×		
Anikeev et al. [7] (2021)	×									×
Ibdah et al. [13] (2021)		×		×	×	×	×			×
Reinhardt et al. [9] (2021)	×		×						×	
Thotawaththa et al. [32] (2021)							×			
Brunotte et al. [14] (2022)		×	×							×
Jesus and Pandit [16] (2022)		×						×		

cess, leveraging a theoretical framework called Protection Motivation Theory (PMT) [1,20] that characterizes the major factors that contribute to people’s attitudes toward protection behavior (attending to their privacy, in our case).

4.3 The Protection Motivation Theory

Our narrative literature review revealed that potential privacy risks and threats of using an application are inefficiently communicated through privacy policies and that we need to explore new design options to motivate users to better respond to these risks and threats when making decisions on selecting the application. Various theoretical frameworks have been adopted to model individuals’ behavior when interacting with information and communication technologies, such as Protection Motivation Theory (PMT) [20,21], theory of

Table 4.2 PMT components illustrated through an analogy of quitting smoking from the previous PMT literature [1] and when adapted to motivate users to attend to privacy.

PMT Component	Motivation to Quit Smoking [1]	Motivation to Attend to Privacy
Maladaptive intrinsic rewards	Bodily pleasure, satisfaction	No need to worry about potential privacy concerns
Maladaptive extrinsic rewards	Social approval	Benefit of instantly using the app features
Perceived vulnerability	Likelihood of contracting a smoking-induced medical condition	Likelihood of the user being affected by not understanding the policy
Perceived severity	Degree of bodily harm, intrapersonal threats like self-esteem, interpersonal threats like family and work relationships	How much the user will be affected by a privacy risk resulting from not understanding the policy
Response Efficacy	Smokers consider stopping smoking to be an effective way to avoid the dangers associated with smoking	Users perceive that adopting a suggested privacy setting is an effective way to avoid privacy risks associated with not understanding the policy
Self Efficacy	Smokers think they can stop smoking	Users are confident to protect their privacy by following the suggested privacy settings
Response Costs	Effort required to stop smoking	Time and effort required to understand the policy

planned behavior [70] and theory of social influence processes [71], among others. Given our study’s focus on the motivational aspect of privacy protection, PMT stands out as an ideal theoretical framework since it specifically addresses users’ protective behaviors in response to threats.

4.3.1 Protection Motivation Theory

Protection Motivation Theory (PMT) is a theoretical framework for understanding how individuals respond to threats and subsequently engage in behaviors to protect themselves [20,21]. According to PMT, individuals engage in a cognitive process of assessing the threat and their ability to cope with it. This process involves two main factors: threat appraisal and coping appraisal.

Threat Appraisal involves an individual’s understanding of the amount of risk posed by engaging in a potentially harmful behavior (i.e., maladaptive response). It is influenced by the following components:

1. Maladaptive Intrinsic rewards – for potentially harmful behavior, the positive feelings or satisfaction an individual experiences when they engage in that behavior;
2. Maladaptive Extrinsic rewards – external reinforcements, provided by other individuals or the environment, that can encourage an individual to engage in a potentially harmful

behavior;

3. Perceived severity – the possible degree of harm resulting from engaging in the potentially harmful behavior;
4. Perceived vulnerability – the probability that the individual will experience harm resulting from engaging in the potentially harmful behavior.

Coping Appraisal, on the other hand, concerns an individual’s assessment of their ability to change the potentially harmful behavior (i.e., adaptive response) and the ability of such a response to alleviate the threat. This factor depends on three components:

1. Response efficacy – an individual’s belief that the adaptive response will truly help avoid the threat;
2. Self-efficacy – an individual’s belief that they are able to carry out the adaptive response to avoid the threat;
3. Response cost – an individual’s belief about how costly (e.g., in terms of money, time, effort) carrying out the adaptive response will be to the individual.

Table 4.2 illustrates PMT through two examples, one on quitting smoking from the previous PMT literature [1] and the other on attending to privacy in the context of our study. Among the PMT components, an increase in perceived severity and vulnerability, response efficacy, and self-efficacy, and a decrease in maladaptive rewards and response costs, can motivate behaviors preventing the threats [21]. Overall, PMT suggests that individuals are more likely to engage in protective behaviors when they perceive the threat as severe and likely to occur, and when they perceive the available coping strategies as effective and feasible.

4.3.2 Applications of PMT in HCI, Security and Privacy

Originally applied to the healthcare domain, PMT and its variations have found numerous applications in fields related to computing, including the study of protective behaviors related to online privacy threats [72–74] and information-sharing and security behaviors [75–82]. PMT has also been applied to develop nudging interventions to encourage users to adopt secure behaviors [83, 84]. Moreover, Chennamaneni and Gupta [85] used PMT to develop a research model to investigate the factors influencing mobile app users’ privacy concerns and their corresponding privacy protection behaviors. Ganesh et al. [86] used PMT as a base to build a 2D persuasive game that instructed users about privacy and security best practices

in smartphones. In our work, we consider PMT as the framework to structure the design ideation and we further used it to assess the impact of the design ideas on users' motivation in a user study.

4.4 Design Process

Following a theory-driven iterative process [19], we proposed a conceptual design for the product page of mobile apps in app stores, in particular, for a hypothetical fitness application as a concrete case study. We first generated design ideas targeting different components in PMT that might impact human motivation when preventing negative outcomes of certain behaviors. We then iteratively created preliminary conceptual designs and refined them by incorporating user feedback from initial user studies.

4.4.1 Case Study Selection

Our study focuses on redesigning the product page for applications in mobile app stores. We selected the iOS Apple Store as our target given the popularity of iOS as a mobile operating system, but the design ideas presented are applicable to other app stores as well, such as Google Play Store. The product page serves as the initial user touchpoint, providing primary information about the application, such as user ratings, key features, categories, etc. Currently, the privacy practices of an application are disclosed under the App Privacy section in the format of privacy labels. These labels are grouped based on whether the data may be used to track an individual across other apps and websites or whether the data is linked to one's identity. We consider the current design of the App Store product page as a baseline and enhance it with more privacy-related information for the application corresponding to the different design categories.

For the conceptual design prototype, we decided to create a mock application in the category of fitness apps. Fitness apps, that encourage users to be physically active, are popular and widely downloaded [87]. However, those apps collect and deal with a large amount of sensitive information, such as biometric data (e.g., heart rate, step count), location data, and personal health information (e.g., weight, diet, sleep patterns). While such information can provide detailed insights into a user's daily routine, health status, and personal habits, the sensitive nature of those data makes fitness apps particularly attractive to hackers and data brokers seeking to exploit it for nefarious purposes [88, 89].

We examined ten popular fitness apps on the App Store (Adidas Running, Apple Health, Asana Rebel, Google Fit, Fitbit, Komoot, FITIV Pulse, Nike Training Club, Peloton, and

Strava) to understand their privacy-sensitive processes. Among them, Strava and Nike Training Club collected the widest variety of personal information, including identifiers, purchase data, usage data, location, health and fitness data, contact information, financial information, and search history, among others. By studying the privacy policies of the two applications in greater detail, as they represent the most severe privacy concerns, we derive the privacy practices for our mock application, named UFit.

4.4.2 Design Ideation

The ideation process started with brainstorming sessions, during which all authors of this work generated and discussed design ideas targeting each component from PMT. We then clustered the ideas into six high-level categories based on the design tactics and further generated multiple design ideas in each category. Table 4.3 summarizes these categories and the design ideas that emerged from brainstorming.

4.4.3 Design Iterations

An iterative approach was followed for the conceptual design of the App Store product page of our mock application UFit. We first developed our initial design ideas presented in Table 4.3 into features using Figma³ for critique and iteration among the authors. We initially created separate features to capture each design idea. We then conducted a user study with three participants to collect early user feedback and further iterate the design. The participants were recruited from our personal network and compensated \$30 CAD. All participants were female and current university students. During the study, we asked their opinions, as potential users of UFit, on the perceived usefulness of each privacy-related feature we proposed, how the features motivate them to understand and protect their privacy, and their other feedback related to the design.

The primary feedback was regarding merging and complementing closely related features, increasing the prominence of features, and avoiding overloading information. We used these insights to make further changes to the design of the conceptual prototype, notably combining the originally separated features into a coherent design. Particularly, we moved the privacy violation cases under the privacy rating page (both related to the *Data & Statistics* category, see Table 4.3) since they are closely related. We also added two prominent buttons on top of the app screenshots to make easy access to the Privacy FAQ (from the *Condensing Information* category) and the Privacy Tutorial (from the *Assistance* category). In addition,

³<https://www.figma.com/>

Table 4.3 Design categories and ideas emerged from the design ideation phase

Category	Description	Related PMT Comp.	Design Ideas
Assistance	Providing assistance and scaffolding to users in managing their information privacy can enhance their confidence and sense of control.	• Self-Efficacy • Response Efficacy	 Introducing “privacy tutorial” to help the user understand how to attend to their information privacy in the application.  Providing flexible options and making it convenient for users to adjust and customize their privacy settings.  Highlighting the available choices and options within the privacy policy to improve user awareness.
Condensing Information	Summarizing the privacy policy and privacy-related information into more relevant and digestible textual formats to reduce information overload	• Response Cost • Response Efficacy	 Using FAQs to summarize the privacy policy and discuss other common privacy-related topics.  Summarizing the privacy policy using plain language and explanations.
Data & Statistics	Presenting privacy-related data and statistics to offer a more concise representation of privacy-related information.	• Perceived Vulnerability • Perceived Severity	 Including “privacy rating” to convey the level of privacy-related risks associated with downloading the app.  Presenting privacy violation cases for similar apps in the category.  Indicating the number of users who viewed or used the opt-out options.
Inhibition	Encouraging or mandating the users to attend to privacy before allowing them to use the app features.	• Maladaptive Rewards	 Prompting the user to first read the privacy policy when clicking the Get button to download the app.  Hiding positive reviews until the privacy policy is read.  Reducing the value of the service until the privacy policy is read.  Requiring a minimum time spent on the privacy policy before download.
Social Interaction	Making users aware of privacy problems in the application through sharing and collaboration.	• Perceived Vulnerability • Perceived Severity • Self-Efficacy	 Showing social signals such as privacy-specific user reviews to emphasize privacy concerns raised by other users.  Allowing users to contribute to the understanding of privacy policies by providing crowd annotations and comments.
Visualization	Simple and intuitive visualizations can convey complex privacy concepts in a more accessible and engaging manner.	• Perceived Vulnerability • Perceived Severity • Response Cost	 Using icons to reduce information overload and aid understanding.  Highlighting the risks and threats in the privacy policy and user reviews  Using visual cues (color, size, etc.) to indicate the severity.  Using comics or fiction to encourage imagining potential privacy risks.

 Ideas emerged from brainstorming and included in our conceptual design

 Ideas emerged from brainstorming but not included in the conceptual design due to feasibility or complexity

we adjusted the feature related to *Inhibition* to direct the user to the Privacy FAQ instead of the original, hard-to-digest privacy policy. Similarly, the design ideas for the categories *Visualization* and *Condensing Information* were combined to link the icons with the information in the FAQ instead of the privacy policy. In the next section, we elaborate on the details of our final design.

4.5 Final Design

The final design of the product page in the App Store incorporated five main features across the six design categories in Table 4.3: (1) *privacy FAQ*, (2) *rating on privacy practice*, (3) *tutorials on customizable options*, (4) *a prompt for users to review privacy FAQ*, and (5) *user reviews related to privacy*. Figure 4.1 illustrates how users can interact with these features when encountering an application.

4.5.1 Privacy FAQ

A prominent red button at the top of the product page directs the user to Privacy FAQ (① in Figure 4.1). This section presents information from the privacy policy [90] and additional information in a compact question-answer format, divided into three main sections, i.e., *Data Collection* (e.g., what type of data is collected and how long is my data stored for), *Third Party Involvement* (e.g., what third parties are involved and can I control what data is shared with third parties), and *User Options* (e.g., what opt-out options are available and can I adjust my settings anytime).

Additionally, each question in the FAQ is annotated with icons representing the following properties of the information: (1) User recommended, indicating a scenario wherein users mark certain sections as important or must-read; (2) Exploitation of data, indicating potential misuse of personal data; and (3) Opt-out options, discussing the options available for a user to opt out of having their personal information collected, shared or used in a certain way. Users can filter information by those properties easily by clicking the corresponding icons on top of the FAQ.

4.5.2 Privacy Rating

Privacy rating mimics the concept of app ratings present in the App Store, serving as an assessment report on the app’s level of adherence to privacy best practices and data protection standards. In our design, the privacy rating is presented next to the app rating in the top bar of the product page. The text indicating the risk level (i.e., high, medium, low) is colored-

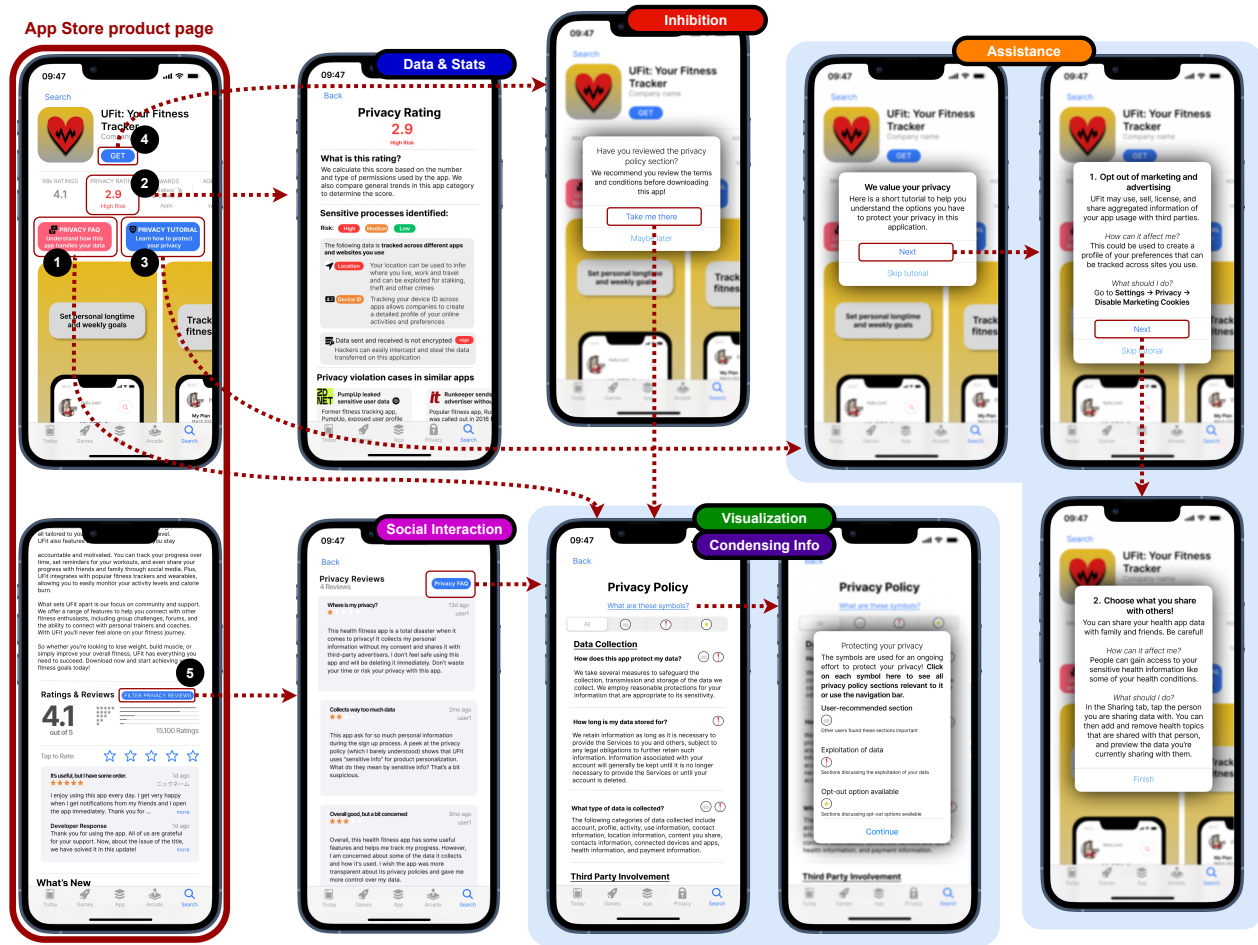


Figure 4.1 Primary features to motivate privacy consideration in our final design, including ① privacy FAQ, ② rating on privacy practice of the app, ③ a short tutorial on customizable privacy options, ④ a prompt for users to review privacy FAQ before downloading the app, and ⑤ user reviews related to privacy.

coded (red, yellow, or green respectively) to draw the user's attention. Clicking on the rating takes the user to a page with more information about the rating (② in Figure 4.1). This page gives a brief description of the privacy rating and lists the sensitive processes (ranked by risk level) contributing to the rating, such as the permissions accessed by the app, information collected and shared with third parties, or questionable privacy practices in the app.

At the bottom of the privacy rating page is a section pertaining to cases of privacy violations in similar applications. Each case is presented in a card containing a title, a brief summary of the incident, and a link to a relevant article or external source. This section aims to help the user get familiar with how their information privacy could be compromised through relevant real-world incidents and therefore contextualize the presented privacy rating.

4.5.3 Privacy Tutorial

The features related to configuring the privacy options in an application are often hard to locate and, even when located, difficult for the users to understand the consequences [9]. The privacy tutorial in our design presents users with guidance on how to take actions related to their information privacy in the app. Our tutorial highlights the primary concerns related to the privacy practices of the app, inspired by the privacy violation cases and common fitness app features. The first part of the tutorial describes how the privacy practice of the app would impact the users; then, it suggests step-by-step instructions on locating and setting the appropriate privacy options to mitigate the risk (see ③ in Figure 4.1).

4.5.4 Privacy Prompt

Most mobile applications today require users to agree to the terms of use and privacy policy after downloading the application, generally during the registration flow. However, it can be beneficial to nudge users towards examining the privacy information of the application before downloading it to help them make more privacy-aware decisions [83,84]. Our design incorporated a pop-up that is displayed when the user clicks the “Get” button to download the application, encouraging the user to visit the Privacy FAQ page before they download the application (④ in Figure 4.1).

4.5.5 Privacy Reviews

User ratings and reviews are among the most important factors that shape the decision-making process of online consumers [91]. While app stores have already integrated user ratings and reviews, the sheer number of reviews left for popular apps makes it challenging to draw users’ attention to reviews concerning privacy. In our design, we included a button under this section to extract the privacy-related reviews (⑤ in Figure 4.1). Clicking on the button takes the user to a page displaying only those reviews sorted in reverse chronological order. A review is classified as privacy-related if it discusses topics such as the permissions used by the application, personal data collected, used, or shared with third parties, and the privacy practices of the application.

4.6 User Study Methods

We conducted a user study to understand the potential impacts of our conceptual design and collect user feedback on specific design ideas. The user study included an online experiment

and a follow-up interview. The Research Ethics Board of all involved institutions approved the study. Below, we outline the data collection and analysis methods for each part of our study.

4.6.1 Online Experiment

We conducted a between-group online experiment to assess the effects of two designs on the privacy awareness and motivation of the participants: (1) our conceptual design of the enhanced App Store product page as shown in Fig. 4.1 (treatment condition) and (2) a mockup of the current iOS App Store design containing the App Privacy section (control condition).

Participants

Participants were recruited from Prolific⁴. Participants had to meet the following criteria to access our study: (1) they can conduct the study in English, (2) they use mobile devices at least 2 to 3 times per day, and (3) they have completed 10 previous Prolific submissions with a minimum acceptance rate of 85%. Each participant was compensated with \$5 CAD.

In total, 87 participants completed the online experiment in the treatment condition and 85 in the control condition. Among the completed submissions, 11 were rejected due to low-quality input (six from the treatment group, and five from the control group). The quality of the input was deemed low if: (1) the participant did not complete a required section of the experiment (such as completing the exploration of the design) or (2) the participant demonstrated low-effort responses (such as one-word answers to all open-ended questions).

Among the remaining 81 treatment group participants and 80 control group participants, around 50% were between 18 and 24 years of age, and approximately 55% were male. The highest proportion of participants had a bachelor's degree in both conditions (51.9% for the treatment condition and 35% for the control condition). A total of 33 participants indicated that they used mobile devices every day, while 128 used mobile devices multiple times every day. The detailed demographics are displayed in Table 4.4.

Experiment procedure

The procedure and material of the experiment (e.g., questionnaire) were refined through multiple rounds of in-person and online pilot studies. During the actual experiment, after

⁴<https://www.prolific.co>

Table 4.4 Participant demographics of the online experiment

		Treatment	Control
Age group	18-24 years	36	41
	25-34 years	31	23
	35-44 years	7	12
	45-54 years	2	4
	55-64 years	4	-
	65+ years	1	-
Gender	Male	44	48
	Female	36	31
	Non-binary / third gender	1	1
Education	Less than high school degree	-	2
	High school graduate	10	25
	Some college / associate degree	19	18
	Bachelor's degree	42	28
	Master's degree	9	6
	Doctoral degree	1	1
Total		81	80

answering demographic questions, participants were asked to consider the scenario of deciding on a fitness app to install and were directed to explore a UFit product page design hosted on Maze⁵. According to the participant's experimental group, either our conceptual design (see Fig. 4.1) or a mockup of the current App Store design was shown to the participant. When the participants indicated that they completed exploring the product page, they were prompted with a message asking them if they had visited all privacy-related sections; the treatment condition prompted a message that links to the four main design concepts (i.e., privacy FAQ, privacy rating, privacy tutorial, and privacy reviews), while in the control condition, this message included a link to the App Privacy section of the page. The prompt was added based on the feedback from the pilot studies to ensure that the participants had the chance to be exposed to privacy-related information *in both conditions*. This study design aligns with our objective to understand whether the proposed design can effectively motivate users, compared with the current App Store design of privacy labels. For the same reason, participants were made aware of the study objective through the study title when giving their consent to join the study.

After exploring the product page design, participants in both conditions were asked to rate their level of agreement on a 5-point Likert scale for five statements, listed in Table 4.5,

⁵<https://maze.co>

Table 4.5 Final PMT statements for online experiment

Statement	Corresponding PMT Comp.
- This design helps me understand the likelihood of privacy-related problems that I could face when using this application.	Perceived Vulnerability
- This design helps me understand the severity of privacy-related problems that I could face when using this application.	Perceived Severity
- The features presented in the design can help me attend to the privacy-related problems in this application.	Response Efficacy
- I am confident that I can take actions to attend to my information privacy in the application through this design.	Self Efficacy
- This design reduces the effort required to attend to my information privacy in this application.	Response Cost

each corresponding to one PMT dimension. For each rating, they were also asked to provide a textual explanation of their rating. The statements were inspired by the work of Chen-namaneni and Gupta [85] and refined through the pilot studies to ensure their clarity; the statement for maladaptive rewards was omitted as the users in our pilot study indicated confusion about the underlying concept. To minimize potential order effects in the study, we implemented a counterbalancing strategy by reversing the sequence of the PMT questions for half the participants in both conditions. After completing an equal number of control and treatment studies with the reversed question order, we did not find a significant difference in the ratings with different question orders. Our data analysis is thus based on the merged samples of questions in original and reversed orders.

Finally, before exiting the experiment, participants were asked to provide overall feedback on the design. They were also asked to state their interest in a follow-up interview. Among the 161 accepted submissions, the median completion time of the experiment was 15.34 minutes.

Data analysis

We conducted a Mann-Whitney U test on each PMT dimension to assess if there was a difference between the treatment group and the control group. Then, for the explanations that the participants provided in both conditions, we conducted an inductive thematic analysis [92] using Atlas.ti to identify themes in participants' positive and negative responses related to the PMT dimensions; the codes and themes were organized by the type of design (i.e., control or treatment). Particularly, two researchers first independently coded the responses from the treatment and control groups. The coding was then discussed among all four authors until any disagreements or concerns were resolved.

4.6.2 Interview

We invited participants who had indicated further interest during the online experiment to participate in a follow-up interview.

Participants

We prioritized recruiting participants who provided high-quality responses during the online experiment – they had descriptive answers in the survey and shared opinions with the prospect of further elaboration. This recruitment method was used to increase the likelihood of gathering more constructive insights. A total of nine participants participated in the interviews: five from the control condition and four from the treatment condition. Four of the interview participants were female and five were male. Their age ranged from 18 to 34. Table 4.6 summarizes the participants.

Interview procedure

All interviews were held on Zoom and were recorded. Each interview lasted around 30 minutes and each participant was compensated with \$15 CAD. We asked them personalized questions about some of their insightful responses to the survey in the online experiment. For example, if a participant suggested an improvement in our design, we would ask them to elaborate on their ideas and rationales. Following that, we asked participants to explore the design prototype they had not seen during the experiment (i.e., participants from the control condition would see the treatment design, and vice versa). We then asked them to rate the PMT questions for the new design and compare it to the original design they saw in the experiment. This interview study thus aimed to enrich our understanding of the rationales behind the participants' online experiment responses and allow us to better compare the potential impacts of both designs.

Data analysis

All interviews were transcribed verbatim. Then, through thematic analysis [92], we refined and enriched the themes identified from the qualitative answers from the online experiment. The codes and themes were used to enrich those that emerged from the survey, as the interview was designed to allow the participants from the online experiment to elaborate on their qualitative responses provided in the survey.

Table 4.6 Participant demographics of the interview

ID	Gender	Age Group	Education	Design tested in online expt.	Weekly device usage
P1	Male	18-24	Bachelor's degree	Control	Every day
P2	Male	18-24	Bachelor's degree	Treatment	Multiple times every day
P3	Female	25-34	Bachelor's degree	Control	Every day
P4	Male	25-34	Bachelor's degree	Control	Multiple times every day
P5	Male	18-24	Bachelor's degree	Control	Multiple times every day
P6	Female	18-24	Some college/ associate degree	Treatment	Multiple times every day
P7	Male	25-34	High school graduate	Control	Every day
P8	Female	25-34	Some college/ associate degree	Treatment	Multiple times every day
P9	Female	18-24	Bachelor's degree	Treatment	Multiple times every day

4.7 User Study Results

Our findings indicate that the treatment design was particularly successful in increasing participants' *Perceived Vulnerability* and *Perceived Severity*, but fell short of reducing *Response Cost*. Participants' qualitative feedback provided useful insights into the reasons behind this outcome. In the sections below, we first report the statistical results of participants' ratings on PMT dimensions and then describe the themes we identified in their feedback on both the control and treatment designs.

4.7.1 Rating on PMT Dimensions

Fig. 4.2 shows the results of the PMT ratings for both the treatment and control designs. For all PMT components, except *Response Cost*, the treatment design received a higher percentage of positive ratings (Agree and Strongly Agree) as compared to the control. The treatment design was most effective in addressing *Perceived Vulnerability* and *Perceived Severity*, as they received the highest number of positive ratings (78.8% and 80.7% respectively); in comparison, the control design received positive ratings of 69.6% and 59.2% for those same categories respectively. However, participants felt that the control design targeted *Response Cost* effectively (71.0% positive ratings) compared to the treatment design (56.3% positive ratings).

Mann-Whitney U tests (with the two-tailed hypothesis and alpha level of 0.5) were carried out for each of the PMT components to compare the results between the treatment and control groups. The tests showed that the differences were statistically significant for *Perceived Severity* ($U = 2521$, $p = 0.015$), *Response Efficacy* ($U = 2128$, $p < 0.001$) and *Self-Efficacy* ($U = 2428$, $p = 0.006$). Meanwhile, the differences between the groups for *Perceived Vulnerability* ($U = 2756$, $p = 0.103$) and *Response Cost* ($U = 2694$, $p = 0.352$) were not significant.

During the interview, the participants were explicitly asked which design they thought was

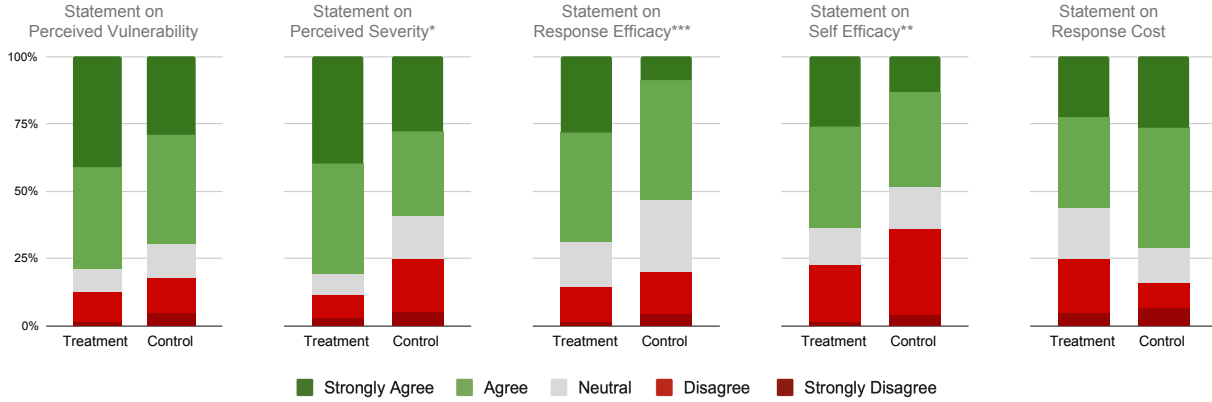


Figure 4.2 Participant ratings for PMT statements. The stars indicate significant differences between the control and the treatment conditions (** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$).

more effective in motivating users to attend to their information privacy. Three participants felt that the control was better in this regard, while the other six participants agreed that the treatment design was more effective. Their reasons align with the themes described below.

4.7.2 User Feedback on the Control Design

Our thematic analysis revealed various themes regarding the positive and negative aspects of the control design (i.e., the original App Store product page with the privacy labels) that affected the participants' perception of the PMT dimensions. The number N after each theme refers to the number of participant comments from the online experiment relating to that theme.

Positive factors about the control design

Concise and simple ($N = 98$): Participants considered the privacy labels included in the App Store to be brief, compact, and straightforward. When discussing *Perceived Vulnerability* and *Perceived Severity*, participants mentioned that “[The design] is compact and to the point” and “the icons are easier to look at than sentences.” The lower amount of text in the design also increased participants' perceived *Response Efficacy* and *Self Efficacy*, as P6 commented during the interview: “The information is summarized and easy to read because you know where to look.” Similarly, the perceived *Response Cost* also decreased; e.g., “Everything is placed in a manner that is easy for the user to analyze those statistics.”

Facilitate informed decision-making ($N = 59$): Participants noted that the privacy labels guided their decision-making process on whether to download the app. For example,

a participant expressed a *Perceived Vulnerability*: “*This design ... makes me aware of just how much data/information the app needs to access. ... Unless I could change these settings in the app I wouldn’t download it.*” Another participant also mentioned when discussing *Perceived Severity*: “*If an app asks for an alarming amount of information access, I can choose not to install it.*” For both *Response Efficacy* and *Self Efficacy*, participants felt that the control design allowed them to understand available privacy-related options, helping them decide how to use the app; for example, “*There seem to be sufficient options related to data collection.*” Participants also mentioned that the control design reduced *Response Cost* of making decisions; e.g., “*You get a good primer on what there is and is a good option for making a preliminary decision.*”

Broad coverage of privacy risks ($N = 52$): Participants thought that the App Store’s app privacy section offered comprehensive information about potential privacy risks associated with using the app. For example, when discussing *Perceived Vulnerability*, a participant mentioned: “*Every data that could get stolen/leaked etc. is mentioned in the app privacy section.*” When talking about *Perceived Severity*, a participant also wrote: “*The design clearly shows me what types of data are used for which purposes and might therefore lead to privacy-related problems I am uncomfortable with.*” Similarly, users felt that the thorough information allowed them to confidently make informed decisions when downloading the app, increasing their *Response Efficacy* and *Self Efficacy*, as a participant indicated: “*being transparent about the data gives me the opportunity to make conscious choices.*”

Negative factors about the control design.

Overly condensed ($N = 61$): Many participants mentioned that the information presented lacks details and clarity, as P9 articulated during the interview, “*It’s just telling you like ‘this may be collected’ but not telling you how to avoid it or any implications of the sensitive information being tracked*”, decreasing *Perceived Vulnerability*. Another participant expressed a lower *Perceived Severity* as the design “*did not explain in detail how severe these different privacy options were.*” A participant also wrote about *Response Efficacy*: “*the design is merely informative and is oblivious to any problems with the application.*” At the same time, participants’ *Self-Efficacy* was negatively affected by the overly condensed information, as a participant explained that “*the next step has to be wading through the privacy agreements... to understand how that data is being gathered and to what end... And this can be a laborious task.*” To improve the design, participants suggested that there should be “*clearer and more lucid descriptions*” that uncover “*what may be hidden by the app developer.*” A participant also specified their information needs: “*I would like to be able to get more inside info as to*

why this kind of data and what for it is going to be collected. How is it related to fitness and in what way does it improve the final product's user experience." Some participants suggested adding Q&As and external sources to address this.

Lack of actionable options and features ($N = 51$): Many participants felt that the privacy section provided information but lacked options to help address their privacy concerns, leading to lower *Response Efficacy* and *Self-Efficacy*. For example, P4 elaborated their concerns regarding the app permissions during the interview: *"When you have an app and you see the rights, you have to allow them all... You can't really disable the ones you are not agreeing with."* P9 from the interview also discussed the insufficiency of using visual summaries such as icons: *"I don't think the icons alone would lead me to take an action... They're just telling you, not really prompting you to do something."* Participants from the survey similarly commented: *"I just don't really see whether I can agree to something or not, it seems like it is demanded by the app."* The concerns are also reflected in the participants' suggestions for improving the design. For example, a participant mentioned that they would prefer if *"It could be noted whether the user can disable some of the app's tracking activities."*

Hidden and lack of visual cues ($N = 16$): Some participants voiced the concern that in the control design, the app privacy information is hidden in the long list of other information about the app. For example, when discussing *Response Cost*, a participant mentioned that *"the average person will not scroll all the way down to read it."* A similar concern was voiced by P6 from the interview: *"It doesn't warn you right at the beginning... So you have to really give the app time and be attentive."* Another participant also mentioned about *Response Efficacy*: *"sometimes we forget to read the smaller words."* Moreover, participants noted higher *Response Cost* due to limited visual cues to help them digest the information; for example: *"The design does not have any visible and attractive branding for privacy-related emergencies that may occur."* Participants recommended, e.g., to include *"more colors to differentiate them from other information"* and *"make the more sensitive parts stand out."*

4.7.3 User Feedback on the Treatment Design

Participants discussed various positive and negative aspects of the treatment design. We first summarize these aspects below; then, we report participants' feedback on each specific design feature.

Positive factors about the treatment design.

The salience of information ($N = 36$): Participants described different aspects concerning

how visible the privacy information is in the treatment design. For example, when discussing *Perceived Vulnerability*, a participant mentioned: “*There are lots of easily seen buttons (Privacy FAQ, Tutorial) that I can see and click to find out more information.*” Some participants also highlighted the use of color-coded texts and icons to convey a sense of risk, which caught their eyes and increased their *Perceived Severity*; e.g., “*Concerning things are in red, which draws my attention and makes me want to find out more;*” and, “*Each part has a symbol to show if there is some risk.*” In the interview, regarding *Response Cost*, P5 said: “*The [treatment design] is easy as ... the info is right there on the front page in the home screen.*”

Navigability ($N = 36$): The easily navigable information had a positive impact on *Response Efficacy* and *Self Efficacy*, as the following response indicates: “*You only have to click a few buttons to have the information at your disposal, making it easier to take action.*” On a similar note, another participant stated, “*Because the privacy section is well organized, browsing and finding a wanted topic becomes more efficient.*” Some participants pointed out how the navigability of the design influenced *Response Cost*; e.g., “*It was easy to reach my ‘information privacy’, so on that part, yes I do agree this design reduced the effort.*”

Detailed information about privacy ($N = 29$): Participants found the design comprehensive in explaining the app’s data practices, privacy risks, and protective measures. For example, when discussing *Perceived Vulnerability*, a participant stated, “*It does a good job explaining why the app could be intrusive within privacy terms.*” Relating to *Perceived Severity*, participants also highlighted that the design conveys the potential consequences of not taking action to safeguard one’s privacy; e.g., “*The reviews and privacy FAQ help me understand how badly my information could be used and how it is all processed.*” Participants acknowledged that the detailed information, particularly through the tutorial, helped them understand the possible actions and increased their perception of *Response Efficacy* and *Self Efficacy*; e.g., “*Provided detailed steps you can take to protect your data such as stopping marketing ads and sharing only certain things with others;*” and “*There is info letting me know how to take action to attend to my information privacy which makes me confident that I can do so.*”

Facilitate informed decision-making ($N = 25$): Participants felt that the treatment design guided their privacy-related decisions in the application. This increased *Response Efficacy*, as a participant explained, “*All information provided help the user to make an educated choice.*” Participants also expressed increased *Self Efficacy*; e.g., “*I, as a user, can take to decide if I want to accept the terms, and I can also choose what I want to share.*” In terms of reducing *Response Cost*, the interview participant P9 elaborated on the benefit of having access to the privacy information before downloading the application: “*Instead of*

having to download the app and then going to the app and checking like ‘OK, these are the privacy things that you should be aware of’, it was already on the interface before I even had to download the app.”

Ability to take action ($N = 10$): Some participants noted how information in the treatment design increased their perception of *Self Efficacy* in attending to their privacy; e.g., *“You only have to click a few buttons to have the information at your disposal, making it easier to take action.”* They also mentioned the ability to control the settings in the app as one important factor; e.g., *“I’m able to change settings about protecting my data while using the app;”* and, *“I can opt-out and choose to be selective of what I share on the app.”*

Negative factors about the treatment design.

Information overload ($N = 15$): While many participants appreciated the amount of detailed information in the design, others felt that the design was too heavy with information that users would not be likely to read. For example, a participant stated, *“If it was an everyday download of the app, I think if I opened the new design [treatment] I would probably not read it...”* The amount of information mainly affected participants’ opinion of the *Response Efficacy*, *Self Efficacy*, and *Response Cost*; e.g., *“Too much information, should be less for the user;”* *“Application provides the option, but it seems way too sophisticated for an average user;”* and, *“The long text can be hard to read through.”* Participants recommended further reducing the text and using alternative formats such as graphs or videos to convey the information.

Fragmented information ($N = 7$): Participants also felt that the privacy information in the design was too scattered. One comment explained, *“Not all available information was easily visible in one place.”* After being introduced to the treatment design, P1 also felt the same during the interview: *“The information is a bit broken apart..., which makes it a bit more difficult to make sure that I have read everything.”* Suggestions proposed by participants included grouping the information to make it easier to identify: *“...I think all things regarding privacy should be kept in one place. I might put it under ‘Privacy rating’, but with red background and here would be all information, FAQs and reviews.”*

Discoverability of certain features ($N = 7$): Some participants were unable to identify the features in the design that were meant to help the user attend to their information privacy. This lowered their opinion of the *Response Efficacy* of the design, as a participant stated: *“I did not see any option that would enable me to attend to the privacy-related problems in this application.”* It also negatively impacted participants’ *Self Efficacy*; e.g., *“The privacy-*

related problems are not addressed on this app. They do not give you an option to not share info.” A participant also suggested adding *“a search bar to find keywords.”*

Feedback related to specific design features

Many participants directly described specific aspects of the five main design features that contributed to their assessment of the application.

The **Privacy Rating** was the most well-received design feature, being mentioned in 45 responses. For example, a participant mentioned how the feature affected their *Perceived Vulnerability*: *“The rating received in particular displays severe lack of security with which my data is handled, allowing me to easily note that my privacy is not of major priority to the developer.”* Concerning *Perceived Severity*, a participant explained, *“The rating allows for quickly noticing what egregious errors authors of the app have made.”* A similar reasoning also influenced participants’ perception of *Response Efficacy*; e.g., *“The privacy rating is an easy way to figure out if an app is safe or if it has a lot of privacy-related problems.”* While some appreciated the informative red color used for the rating, others desired more prominence; e.g., regarding *Response Costs*, a participant wrote: *“Both ‘Privacy FAQ’ and ‘Privacy Tutorial’ are easily visible but despite the red color I didn’t notice ‘privacy rating.’”*

The **Privacy Reviews** were mentioned in 30 comments, with participants appreciating the input from actual application users; e.g., *“I like the transparency because it showed the privacy reviews from individuals.”* The user reviews helped increase *Perceived Vulnerability* and *Perceived Severity*, as a participant commented, *“Just read the reviews and make my own decision – if I see that the app has a low score in terms of privacy, I’m immediately on the back foot.”* Some participants felt a greater sense of involvement with the application (and hence *Self Efficacy*) through the privacy review feature; e.g., *“Thanks to this function I can read reviews and also give my own so I feel like I can contribute.”* However, some participants questioned the necessity of separating privacy-specific reviews from regular ones; e.g. *“Privacy ‘user ratings’ feel unnecessary - as anyone can write what they feel anytime in regular ratings.”*

The information in the **Privacy FAQ** is referred to in 29 comments. This feature helped participants get a better sense of the anticipated privacy-related problems (i.e., *Perceived Vulnerability* and *Perceived Severity*); e.g., *“In the privacy FAQ we can see how the app manages our data to third party companies or apps that could ask for our data, in that case, we can understand the problems it could bring...”* Some participants viewed the FAQ as a guide to their information privacy, augmenting *Self Efficacy*; e.g., *“Shows you the question and answer section where you can guide yourself.”* P6 from the interview also highlighted that the

FAQ was easily accessible: *“It’s very informative and you can easily find the frequently asked questions so meaning that you can also maybe probably get help right there.”* Contrastingly, some participants indicated that the FAQ could be further condensed, with a suggestion for *“a TLDR at the start/end of the text.”*

Participants mentioned the **Privacy Tutorial** in 24 comments. They appreciated its simplicity and succinctness, as evident in this comment: *“The privacy tutorial is clear and easy to understand and straight to the point”*, improving their perceived *Self Efficacy*. They also denoted the support for *Response Efficacy*; e.g., *“In the privacy tutorial we get step by step how to change the information privacy.”* A participant particularly noted that the completeness of the information in the tutorial influenced their *Perceived Vulnerability* and *Perceived Severity*: *“Everything is said on the privacy tutorial. I like that about the app.”* Some other participants, however, suggested a format improvement, for example, to have *“a video in the privacy tutorial with the step-by-step to change our preferences.”*

Although the majority of the participants clicked the “Get” button, which triggered the **Privacy Prompt**, only one participant mentioned this specific prompt in the comments, in relation to their *Perceived Vulnerability*: *“It was very obvious that privacy issues were highlighted; there were prompts to check the security info before getting the app.”* Some participants also suggested incorporating different kinds of prompts, like *“a pop up that says App Store doesn’t recommend due to privacy concerns”* or *“a little pop up once in a while to remind users of the privacy information”* within the application.

4.8 Discussion

Our conceptual design reimagines the familiar App Store interface in terms of design elements concerning privacy-related information. Using PMT, we specifically addressed the motivational issue of users’ engagement with privacy notices, rather than solely enhancing the representation of the information (e.g., [13,29]). While some of the design ideas have been approached in previous work, such as privacy rating [93], icons and visual cues [13,94], and condensed information [29,95], our work offers a systematic way to consider those ideas in a design space characterized by the PMT components. Results from our user study indicated the intricate relationship between the design ideas targeting different components of PMT and how they collectively impacted users’ motivation. Below, we first reflect on the impact of PMT and our design decisions on user motivation, then we discuss the practical implications of our design and the limitations of our study.

4.8.1 Design Considerations for Motivating Users to Attend to Privacy

Targeting PMT components in combination to induce motivation

During our design process, we discovered that the PMT components interact with each other to promote user motivation; for the threat appraisal to serve a meaningful purpose, users need to be provided with an effective recourse and mechanism to combat the threat (therefore, an increased *Coping Appraisal*). Similarly, for users to be motivated to undertake a protective action, they need a driving factor, such as a clear understanding of the risks posed by a privacy-related problem (related to the *Threat Appraisal*). Similar trends were observed in previous studies, for example, prior victims of social media harms displayed increased safety protection behavior [73], individuals informed of card fraud threats were more likely to use secure mobile payments [83], and showing educational videos about security risks of smartphones without screen locks increased the tendency of users to adopt screen locks [77]. Moreover, in our conceptual prototype, even though each design idea was made to address a few specific PMT components, our participants correlated them to other threats and coping mechanisms as well. For instance, the privacy rating was meant to target *Perceived Vulnerability* and *Perceived Severity* by giving the user a sense of the risk associated with the app. But our participants felt that it also offered an easy solution to judge the safety of the application and avoid downloading it, as a participant commented, “*The privacy rating is an easy way to figure out if an app is safe or if it has a lot of privacy-related problems*”, thus influencing their perception of *Response Efficacy* and *Response Costs*. Therefore, an efficient design needs to integrate and address the PMT components as a whole rather than individually. This was also one of the factors that motivated our decision to merge our preliminary design ideas targeting the PMT components separately into one unified design.

Deciding on the amount and types of information to communicate

While our design has much less text than the standard privacy policy, some participants still felt it daunting to process all the information in this succinct form. This explains the lower ratings for *Response Cost* for our conceptual design. On the other hand, participants indicated that the information provided by privacy labels in the current App Store lacks sufficient details and actionable insights; as a result, participants did not feel confident to take appropriate actions to attend to their privacy in the application (contributing to low *Self Efficacy*). Thus, deciding on the amount and types of information to communicate is crucial to motivate users to examine privacy-related concerns and also enable them to gain meaningful and actionable insights. For future iterations of our design, we need to further

refine the information presentation (and thus reduce *Response Cost*) while maximizing the utility of the information. A perhaps more viable way is to cater to the information needs of different users by providing personalized interfaces.

Using visual cues to make privacy-related information more prominent

During the user study, we noticed that the presentation of the components that we added was very important in highlighting certain PMT components. For example, participants perceived a greater sense of severity and vulnerability on seeing the red color of the privacy rating. Additionally, based on the participants’ feedback, the position of the FAQ and privacy tutorial options played an important role in enhancing their *Perceived Severity* and *Perceived Vulnerability*; this design mitigates a common problem that privacy policies are often inconsistently placed [8]. Therefore, augmenting specific design strategies with strong visual cues, such as the use of color and positioning, can be helpful in enhancing the effect of the design ideas derived from PMT.

Anchoring familiar design ideas to improve user reception and engagement

We intentionally designed the five main features with elements familiar to users to reduce the learning curve and potential hesitation towards unfamiliar concepts. In our study, the privacy rating received the highest number of mentions, followed by the privacy reviews. A possible explanation is that users were able to identify and relate these features to existing App Store features (i.e., the Ratings and Reviews section). It is also consistent with users’ routine to consult the app rating and user reviews before downloading, as indicated by some participants. On the other hand, the privacy prompt was barely mentioned, suggesting that users do not consider it as a separate feature when interacting with the prompt. This resembles common user behavior to “mechanically” click the accept or OK button on privacy policy prompts [12]. Overall, our results showed that users tend to engage with elements they have experience with. These patterns can be leveraged to design interfaces that nudge users to visit targeted sections.

4.8.2 Practical Implications of Our Design

Our study focuses on proposing and validating design concepts rather than suggesting the implementation details of the design ideas. We acknowledge the potential complexity associated with translating these design ideas into complete functionalities. For instance, finding a reliable and standardized method to calculate the privacy rating can be challenging. Our

current design integrates one overall privacy rating calculated according to the application’s privacy practice. However, assessing the level of risk can be a subjective judgment and can vary from user to user. Techniques using user preference when calculating the privacy rating (e.g., [93, 96]) can be considered to overcome this concern. This requires the App Store to integrate mechanisms to explicitly capture the users’ privacy profile or preferences.

For displaying the privacy violation cases in similar apps, there can be a dataset of news articles and reports labeled by app category and further divided into subcategories (e.g., articles related to fitness tracker apps in the category of “Health and fitness”). Then different strategies can be applied to retrieve the most relevant privacy violation cases for a particular application, such as considering the severity of the incident and the correlation with the privacy practices of the application. However, the task of identifying a suitable authority to oversee the ongoing maintenance and expansion of this dataset is a challenge. Integrating crowdsourcing approaches, such as ToS;DR⁶, can also be a valuable alternative.

The current advances in natural language processing (NLP) techniques offer a promising avenue to achieve many proposed features with minimal manual effort, such as identifying the privacy reviews from the pool of user reviews (e.g., [97]) and generating answers to common privacy questions (e.g., [95, 98]). Automated approaches based on NLP may also help address the current practice that requires app developers to self-report their data practices, sometimes leading to misrepresentation [99]. However, the accuracy of the automated techniques requires further examination. Moreover, how to incorporate those techniques in the workflow of privacy information validation needs future investigation.

Additionally, the privacy tutorial informs users of steps they can take to modify the privacy settings or other opt-out options available in the application. However, the coping mechanisms largely depend on the implementation by the developers themselves. The extent and ease of adopting these options may also vary from application to application. The memorability of the presented steps is another limitation of our current design, as there is no easy way for the user to follow the tutorial once the application is launched. Previous work, such as privacy assistants that help the users effectively choose the appropriate settings [100, 101] and contextualizing privacy policy during interaction [102], points to useful directions.

Finally, we acknowledge Solove’s [51] argument that people cannot be fully engaged in privacy self-management given the large number of applications and services users interact with. Solove differentiated “privacy” in a concrete context when people are reasoning the risk of their behavior from the general attitude towards “privacy”. This distinction is also what we advocate in this work. We hope to motivate users to attend to concrete information related

⁶<https://tosdr.org>

to the privacy practices of a certain application, helping them better reason the risks and their vulnerability and gain self-efficacy. In particular, self-efficacy in PMT directly helps to combat the feeling of futility of “privacy self-management.” We also agree with Solove that a bigger impact requires “regulating the architecture that structures the way information is used, maintained, and transferred” [51] so that self-efficacy can sustain. Our current work, however, approaches this from a different angle, motivating users to start to attend to privacy. Such a bottom-up effort (i.e., coming from users) may contribute to accelerating the top-down approach (i.e., coming from regulations) of architectural change.

4.8.3 Limitations and Future Work

Given how our study was conducted, there are several limiting factors to consider. Firstly, we acknowledge that our design focuses on motivating users to understand privacy concerns when they encounter individual apps rather than comparing several competing apps from the same category. Our work currently also does not convey the common privacy practice of apps from one category. However, the scenario we considered in our study often occurs when users select apps to fulfill their needs, which is an important opportunity for educating users about privacy concerns. The application of our findings to broader app categories or user contexts needs to be explored in future work.

Second, in the user studies, we did not conceal from the participants the purpose of the study (i.e., to investigate design principles that address users’ privacy-related motivation). This could have introduced some bias in their interactions with the designs and the type of information they looked for. However, as discussed in Section 4.6.1, this helped to ensure that the participants were equally exposed to the design features and is aligned with our research objective. Moreover, the phrases and examples used in the conceptual design could have also affected participants’ sensitivity to privacy issues and matters. While these phrases and examples were inspired by use cases and possible risks of health apps in real life to provide plausible information to the users, the users’ reactions to different tones and phrasing of similar privacy information should be investigated in future work.

Next, the selective recruitment of interview participants based on the quality of their responses may inadvertently favor individuals who are already more engaged or interested in the topic and may overlook the perspectives and behaviors of less motivated users. This may influence the applicability and generalizability of the study’s conclusions to the broader user population. In addition, the primary way of measuring the motivation of our participants was through self-reporting based on the survey and the interview. However, the feedback participants gave may not reflect their true motivation and associated further actions. More-

over, motivation changes can occur over time and this change was not captured by our study. A longitudinal field study can be conducted in the future to address this. Lastly, since the study was conducted in English and required a certain level of device exposure, we had to filter out potential participants who did not fit these criteria through Prolific. Future work could focus on privacy-related motivation issues of users who use other languages, from other cultures, or who have different technology proficiencies.

4.9 Conclusion

Past work has focused on improving the presentation of privacy-related information but demonstrated limited effort in systematically addressing mechanisms for enhancing user motivation in privacy awareness and action. To address this gap, we utilized the Protection Motivation Theory (PMT) to inform design ideas aimed at motivating users to increase their interaction with privacy-related information. We put these design ideas into a new conceptual design of the App Store interface and evaluated it in a user study. The results indicated that to effectively promote user motivation, PMT components need to be consolidated and the quantity and types of information communicated in design should be carefully considered, and possibly personalized. Moreover, combining PMT-inspired concepts with other design elements, such as visual cues and user familiarity, can yield favorable outcomes. Our research contributes to design considerations and implications that address the essential motivational issue of augmenting users' privacy awareness and enabling users to take concrete privacy protection actions.

CHAPTER 5 CONCLUSION

With our heavy dependence on technology in today’s world, every individual inadvertently shares large amounts of their personal information with the myriad of applications that they interact with in their daily lives. This status quo makes it challenging for users of software applications to protect their privacy from organizations, entities, and individuals seeking to take advantage of their personal data or to use it for malicious purposes such as theft or cyberbullying. Furthermore, privacy policy, as the current primary medium of communicating privacy-related information about an application or service to users, presents various limitations that hinder its utility as an effective informational interface. Thus, users face a major setback with regard to privacy awareness and privacy management. In this thesis, we work towards understanding and addressing this fundamental problem, aiming to empower users to attend to their information privacy.

5.1 Summary of Works

In this thesis, we first sought to obtain a deep understanding of users’ privacy attitudes and perspectives (Chapter 3), by analyzing a sample of 313 privacy-related discussions fetched from the Q&A platform, Quora. We performed an inductive analysis of the questions and answers, extracting discussion aspects such as the privacy topics covered, the types of questions asked, and the characteristics of the responses. We discovered that the questions mainly sought out users’ opinions on privacy-related subjects, with discussions predominantly focusing on topics such as privacy-protecting strategies (particularly secure applications) and privacy risks and dangers (particularly tracking and information leaks). Furthermore, users expressed diverse emotions in their responses, supporting their responses with examples and personal experiences. Our study reveals the multifaceted yet personal nature of privacy that often leaves users with a sense of helplessness and despair. It underscores the importance of collective experience sharing to help users navigate the complex privacy landscape. We also compare our findings to prior works on developer discussions in online forums, highlighting the similarities and differences between perspectives of these two groups.

With the information gathered from the first study, we then honed our focus on the issue of motivating users to attend to their information privacy through a theory-driven design study (Chapter 4). Using the Protection Motivation Theory (PMT) as a base, we formulated design ideas centered around increasing user motivation to interact with privacy-related information, which we refined and developed into a conceptual design prototype of the product page

for a hypothetical fitness tracking application in the Apple App Store. Through an online experiment and interviews, we evaluated the impact of our design in comparison with the current App Store interface involving privacy labels. The results of our study revealed that our design was effective in increasing participants’ perceived vulnerability and severity to privacy threats in the application, thus successfully targeting the main PMT components. Our study yielded valuable design considerations that can inform the design of motivational privacy interfaces, including collectively targeting PMT components, balancing the amount and type of information, employing visual cues for information salience, and utilizing familiar design concepts to enhance user acceptance and engagement.

5.2 Limitations & Future Work

The two studies in our work have several limitations to take into account, which are discussed in detail in the respective chapters (Sections 3.3.3 and 4.8.3). In addition, some other limiting factors and opportunities for future research are considered below.

Firstly, our work is restricted to the English language, and probably the Western culture. In the first study, we only analyzed English-language discussions on Quora. In the second study, one of our criteria for the user study involved knowledge of the English language. These constraints may have limited the diversity of our participants’ backgrounds. However, individuals’ perceptions and attitudes toward privacy can be greatly influenced by cultural and socioeconomic factors [103]. Various studies have explored the cross-cultural dimension of privacy in specific contexts, including social media usage [104, 105], consumer behavior [106], and privacy legislation [107], among others. These studies mainly employed online surveys or interviews to gather data. Examining privacy-related discussions in alternate-language online forums or forums popular in particular countries or cultures may provide a rich opportunity to gain a broader understanding of how privacy concerns vary across different cultures and linguistic groups. These insights can help to develop more inclusive and effective privacy communication strategies that address the unique needs and concerns of a global user base. In particular, Quora supports a number of languages, in turn, fostering diverse, language-specific communities to exchange ideas. For example, Das et al. [45, 108] studied the Bengali version of Quora to understand the effects of colonization on identity formation.

Furthermore, Section 4.8.2 discusses several practical implications of the design ideas proposed in the second study. In particular, one major challenge in designing privacy interfaces is accommodating the varying privacy preferences of individuals. As highlighted in Section 3.7.2, privacy is a subjective and personal experience for users, varying from one individual to another. Future research should explore ways to design privacy interfaces that effectively

accommodate diverse user preferences to further enhance engagement with privacy-related information. Adaptive, personalized interfaces can be investigated to meet users' individual needs.

Overall, our work contributes to addressing the important issue of technology users' privacy awareness. We enriched the understanding of how technology users collectively make sense of the complexity of privacy and provided promising design-oriented solutions to encourage users to manage their personal information more attentively. Our investigation informs future research to be focused on a broader context of users' perception of privacy, considering the diversity of user groups and individual needs.

REFERENCES

- [1] R. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation," *Social Psychology: A Source Book*, vol. 1, pp. 153–176, 1983.
- [2] G. of Canada, "Canada's privacy act," 2021. [Online]. Available: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/pa-lprp.html>
- [3] OECD, "Oecd guidelines for multinational enterprises on responsible business conduct," 2023. [Online]. Available: <https://www.oecd-ilibrary.org/content/publication/81f92357-en>
- [4] European Parliament and Council of the European Union, "General data protection regulation," 2016. [Online]. Available: <https://gdpr-info.eu>
- [5] F. Schaub, R. Balebako, and L. F. Cranor, "Designing effective privacy notices and controls," *IEEE Internet Computing*, vol. 21, no. 3, pp. 70–77, 2017.
- [6] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society*, vol. 4, no. 3 (2008), 543-568., vol. 4, 2008.
- [7] M. Anikeev, H. Shulman, and H. Simo, "Privacy policies of mobile apps - a usability study," in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. New York, NY: Institute of Electrical and Electronics Engineers, 2021, pp. 1–2.
- [8] M. A. A. Robert W. Proctor and K.-P. L. Vu, "Examining usability of web privacy policies," *International Journal of Human-Computer Interaction*, vol. 24, no. 3, pp. 307–328, 2008. [Online]. Available: <https://doi.org/10.1080/10447310801937999>
- [9] D. Reinhardt, J. Borchard, and J. Hurtienne, "Visual interactive privacy policy: The better choice?" in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: ACM, 2021. [Online]. Available: <https://doi.org/10.1145/3411764.3445465>
- [10] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A "nutrition label" for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and*

- Security*, ser. SOUPS '09. New York, NY, USA: ACM, 2009. [Online]. Available: <https://doi.org/10.1145/1572532.1572538>
- [11] A. Adhikari and R. Dewri, “Towards change detection in privacy policies with natural language processing,” in *2021 18th International Conference on Privacy, Security and Trust (PST)*. New York, NY: Institute of Electrical and Electronics Engineers, 2021, pp. 1–10.
 - [12] S. Talib, S. M. Abdul Razak, A. Olowolayemo, M. Salependi, N. F. Ahmad, S. Kunhamoo, and S. K. Bani, “Perception analysis of social networks’ privacy policy: Instagram as a case study,” in *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*. New York, NY: Institute of Electrical and Electronics Engineers, 2014, pp. 1–5.
 - [13] D. Ibdah, N. Lachtar, S. M. Raparathi, and A. Bacha, ““why should i read the privacy policy, i just need the service”: A study on attitudes and perceptions toward privacy policies,” *IEEE Access*, vol. 9, pp. 166 465–166 487, 2021.
 - [14] W. Brunotte, L. Chazette, L. Kohler, J. Klunder, and K. Schneider, “What about my privacy?helping users understand online privacy policies,” in *Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering*, ser. ICSSP’22. New York, NY, USA: ACM, 2022, p. 56–65. [Online]. Available: <https://doi.org/10.1145/3529320.3529327>
 - [15] J. Becker, M. Heddier, A. Öksüz, and R. Knackstedt, “The effect of providing visualizations in privacy policies on trust in data privacy and security,” in *2014 47th Hawaii International Conference on System Sciences*. New York, NY: Institute of Electrical and Electronics Engineers, 2014, pp. 3224–3233.
 - [16] V. Jesus and H. J. Pandit, “Consent receipts for a usable and auditable web of personal data,” *IEEE Access*, vol. 10, pp. 28 545–28 563, 2022.
 - [17] K. Ghazinour and T. Albalawi, “A usability study on the privacy policy visualization model,” in *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)*. New York, NY: Institute of Electrical and Electronics Engineers, 2016, pp. 578–585.

- [18] K. J. Bigrigg and M. W. Bigrigg, “Active dissection of privacy policies: Why johnny doesn’t read privacy policies,” *SIGCAS Comput. Soc.*, vol. 46, no. 4, p. 5–11, jan 2017. [Online]. Available: <https://doi.org/10.1145/3040489.3040491>
- [19] P. J. Cash, “Developing theory-driven design research,” *Design Studies*, vol. 56, pp. 84–119, 2018. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0142694X18300140>
- [20] R. W. Rogers, “A protection motivation theory of fear appeals and attitude change1,” *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.
- [21] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, “A meta-analysis of research on protection motivation theory,” *Journal of applied social psychology*, vol. 30, no. 2, pp. 407–429, 2000. [Online]. Available: <https://doi.org/10.1111/j.1559-1816.2000.tb02323.x>
- [22] J. B. Gross and M. B. Rosson, “End user concern about security and privacy threats,” in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, ser. SOUPS ’07. New York, NY, USA: Association for Computing Machinery, 2007, p. 167–168. [Online]. Available: <https://doi.org/10.1145/1280680.1280711>
- [23] D. C. Nguyen, E. Derr, M. Backes, and S. Bugiel, “Short text, large effect: Measuring the impact of user reviews on android app security & privacy,” in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 555–569.
- [24] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, “Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences,” *Journal of Computer-Mediated Communication*, vol. 15, no. 1, pp. 83–108, 10 2009. [Online]. Available: <https://doi.org/10.1111/j.1083-6101.2009.01494.x>
- [25] H. Xu, X. R. Luo, J. M. Carroll, and M. B. Rosson, “The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing,” *Decision Support Systems*, vol. 51, no. 1, pp. 42–52, 2011. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167923610001983>
- [26] Z. Li, M. Sihag, N. Arony, J. Junior, T. Phan, N. Ernst, and D. Damian, “Narratives: the unforeseen influencer of privacy concerns,” in *2022 IEEE 30th International Requirements Engineering Conference (RE)*. Los Alamitos, CA, USA: IEEE Computer Society, aug 2022, pp. 127–139. [Online]. Available: <https://doi.ieeecomputersociety.org/10.1109/RE54965.2022.00018>

- [27] J. Li, K. Sun, B. S. Huff, A. M. Bierley, Y. Kim, F. Schaub, and K. Fawaz, ““it’s up to the consumer to be smart”: Understanding the security and privacy attitudes of smart home users on reddit,” in *2023 IEEE Symposium on Security and Privacy (SP)*, 2023, pp. 2850–2866.
- [28] J. Pierce, S. Fox, N. Merrill, R. Wong, and C. DiSalvo, “An interface without a user: An exploratory design study of online privacy policies and digital legalese,” in *Proceedings of the 2018 Designing Interactive Systems Conference*, ser. DIS ’18. New York, NY, USA: ACM, 2018, p. 1345–1358. [Online]. Available: <https://doi.org/10.1145/3196709.3196818>
- [29] N. Tomuro, S. Lytinen, and K. Hornsberg, “Automatic summarization of privacy policies using ensemble learning,” in *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, ser. CODASPY ’16. New York, NY, USA: ACM, 2016, p. 133–135. [Online]. Available: <https://doi.org/10.1145/2857705.2857741>
- [30] S. Wilson, F. Schaub, F. Liu, K. M. Sathyendra, D. Smullen, S. Zimmeck, R. Ramanath, P. Story, F. Liu, N. Sadeh, and N. A. Smith, “Analyzing privacy policies at scale: From crowdsourcing to automated annotations,” *ACM Trans. Web*, vol. 13, no. 1, dec 2018. [Online]. Available: <https://doi.org/10.1145/3230665>
- [31] S. Wilson, F. Schaub, R. Ramanath, N. Sadeh, F. Liu, N. A. Smith, and F. Liu, “Crowdsourcing annotations for websites’ privacy policies: Can it really work?” in *Proceedings of the 25th International Conference on World Wide Web*, ser. WWW ’16. Republic and Canton of Geneva, CHE: International World Wide Web Conferences Steering Committee, 2016, p. 133–143. [Online]. Available: <https://doi.org/10.1145/2872427.2883035>
- [32] T. Thotawatththa, Y. Gamage, D. Gamlath, W. Chee, and D. Meedeniya, “Automated categorization of privacy policies based on user perspective,” in *2021 10th International Conference on Information and Automation for Sustainability (ICIAfS)*. New York, NY: Institute of Electrical and Electronics Engineers, 2021, pp. 54–59.
- [33] M. Tahaei, K. Vaniea, and N. Saphra, “Understanding privacy-related questions on stack overflow,” in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–14. [Online]. Available: <https://doi.org/10.1145/3313831.3376768>

- [34] T. Li, E. Louie, L. Dabbish, and J. I. Hong, “How developers talk about personal data and what it means for user privacy: A case study of a developer forum on reddit,” *Proc. ACM Hum.-Comput. Interact.*, vol. 4, no. CSCW3, jan 2021. [Online]. Available: <https://doi.org/10.1145/3432919>
- [35] M. Tahaei, T. Li, and K. Vaniea, “Understanding privacy-related advice on stack overflow,” *Proceedings on Privacy Enhancing Technologies*, vol. 2022, no. 2, pp. 114–131, 2022. [Online]. Available: <https://doi.org/10.2478/popets-2022-0038>;<https://tuliplab.org/papers/tahaei2022pets.pdf>
- [36] J.-H. Hoepman, “Privacy design strategies,” in *ICT Systems Security and Privacy Protection*, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 446–459.
- [37] J. Parsons, M. Schrider, O. Ogunlela, and S. Ghanavati, “Understanding developers privacy concerns through reddit thread analysis,” 2023.
- [38] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman, and A. Balissa, “Privacy by designers: software developers’ privacy mindset,” in *Proceedings of the 40th International Conference on Software Engineering*, ser. ICSE ’18. New York, NY, USA: Association for Computing Machinery, 2018, p. 396. [Online]. Available: <https://doi.org/10.1145/3180155.3182531>
- [39] M. Tahaei, A. Frik, and K. Vaniea, “Privacy champions in software teams: Understanding their motivations, strategies, and challenges,” in *CHI ’21: CHI Conference on Human Factors in Computing Systems, Virtual Event / Yokohama, Japan, May 8-13, 2021*, Y. Kitamura, A. Quigley, K. Isbister, T. Igarashi, P. Bjørn, and S. M. Drucker, Eds. ACM, 2021, pp. 693:1–693:15.
- [40] M. Tahaei, R. Abu-Salma, and A. Rashid, “Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI 2023, Hamburg, Germany, April 23-28, 2023*, A. Schmidt, K. Väänänen, T. Goyal, P. O. Kristensson, A. Peters, S. Mueller, J. R. Williamson, and M. L. Wilson, Eds. ACM, 2023, pp. 168:1–168:24.
- [41] Quora Business. (2023) Reach over 400 million monthly unique visitors on quora. [Online]. Available: <https://business.quora.com/resources/reach-over-400-million-monthly-unique-visitors-on-quora/>

- [42] S. Maity, A. Kharb, and A. Mukherjee, “Language use matters: Analysis of the linguistic structure of question texts can characterize answerability in quora,” *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 11, no. 1, pp. 612–615, May 2017. [Online]. Available: <https://ojs.aaai.org/index.php/ICWSM/article/view/14947>
- [43] S. Patil and K. Lee, “Detecting experts on quora: by their activity, quality of answers, linguistic characteristics and temporal behaviors,” *Social Network Analysis and Mining*, vol. 6, no. 1, p. 5, 2015. [Online]. Available: <https://doi.org/10.1007/s13278-015-0313-x>
- [44] B. Mathew, R. Dutt, S. K. Maity, P. Goyal, and A. Mukherjee, “Deep dive into anonymity: Large scale analysis of quora questions,” in *Social Informatics*, I. Weber, K. M. Darwish, C. Wagner, E. Zagheni, L. Nelson, S. Aref, and F. Flöck, Eds. Cham: Springer International Publishing, 2019, pp. 35–49.
- [45] D. Das and B. Semaan, “Collaborative identity decolonization as reclaiming narrative agency: Identity work of bengali communities on quora,” in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: <https://doi.org/10.1145/3491102.3517600>
- [46] —, “quoras: A python api for quora data collection to increase multi-language social science research,” in *Companion Publication of the 2020 Conference on Computer Supported Cooperative Work and Social Computing*, ser. CSCW ’20 Companion. New York, NY, USA: Association for Computing Machinery, 2020, p. 251–256. [Online]. Available: <https://doi.org/10.1145/3406865.3418333>
- [47] F. Ricca and P. Tonella, “Web site analysis: Structure and evolution,” in *2013 IEEE International Conference on Software Maintenance*. Los Alamitos, CA, USA: IEEE Computer Society, oct 2000, p. 76. [Online]. Available: <https://doi.ieeecomputersociety.org/10.1109/ICSM.2000.883017>
- [48] J. Saldana, *The Coding Manual for Qualitative Researchers*. SAGE Publications, 2015. [Online]. Available: <https://books.google.ca/books?id=ZhxiCgAAQBAJ>
- [49] N. Denzin and Y. Lincoln, *Strategies of Qualitative Inquiry*, ser. Handbook of qualitative research. Sage Publications, 2008. [Online]. Available: <https://books.google.ca/books?id=hD7W095U66cC>

- [50] K. Holtzblatt and H. Beyer, “6 - the affinity diagram,” in *Contextual Design (Second Edition)*, second edition ed., ser. Interactive Technologies, K. Holtzblatt and H. Beyer, Eds. Boston: Morgan Kaufmann, 2017, pp. 127–146. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780128008942000065>
- [51] D. J. Solove, “The myth of the privacy paradox,” *SSRN Electronic Journal*, 2020. [Online]. Available: <http://dx.doi.org/10.2139/ssrn.3536265>
- [52] A. Esteve, “The business of personal data: Google, Facebook, and privacy issues in the EU and the USA,” *International Data Privacy Law*, vol. 7, no. 1, pp. 36–47, 03 2017. [Online]. Available: <https://doi.org/10.1093/idpl/ipw026>
- [53] S. Egelman, “My profile is my password, verify me! the privacy/convenience tradeoff of facebook connect,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 2369–2378. [Online]. Available: <https://doi.org/10.1145/2470654.2481328>
- [54] B. D. Weinberg, G. R. Milne, Y. G. Andonova, and F. M. Hajjat, “Internet of things: Convenience vs. privacy and secrecy,” *Business Horizons*, vol. 58, no. 6, pp. 615–624, 2015, sPECIAL ISSUE: THE MAGIC OF SECRETS. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0007681315000865>
- [55] R. S. Laufer and M. Wolfe, “Privacy as a concept and a social issue: A multidimensional developmental theory,” *Journal of social Issues*, vol. 33, no. 3, pp. 22–42, 1977.
- [56] T. Wang, T. D. Duong, and C. C. Chen, “Intention to disclose personal information via mobile applications: A privacy calculus perspective,” *International Journal of Information Management*, vol. 36, no. 4, pp. 531–542, 2016. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0268401215300797>
- [57] D. Kim, K. Park, Y. Park, and J.-H. Ahn, “Willingness to provide personal information: Perspective of privacy calculus in iot services,” *Computers in Human Behavior*, vol. 92, pp. 273–281, 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0747563218305570>
- [58] V. Shiri, M. Xiong, J. Cheng, and J. L. Guo, “Motivating users to attend to privacy: A theory-driven design study,” in *Proceedings of the 2024 ACM Designing Interactive Systems Conference*, ser. DIS '24. New York, NY, USA:

- Association for Computing Machinery, 2024, p. 258–275. [Online]. Available: <https://doi.org/10.1145/3643834.3661544>
- [59] R. F. Baumeister and M. R. Leary, “Writing narrative literature reviews,” *Review of General Psychology*, vol. 1, no. 3, pp. 311–320, 1997. [Online]. Available: <https://doi.org/10.1037/1089-2680.1.3.311>
- [60] B. N. Green, C. D. Johnson, and A. Adams, “Writing narrative literature reviews for peer-reviewed journals: secrets of the trade,” *Journal of Chiropractic Medicine*, vol. 5, no. 3, pp. 101–117, 2006. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0899346707601426>
- [61] G. Scholar, “Human-computer interaction – google scholar metrics,” 2024. [Online]. Available: https://scholar.google.ca/citations?view_op=top_venues&hl=en&vq=eng_humancomputerinteraction
- [62] H. Singh and M. Bhusry, “Privacy policy inference of multiple user-uploaded images on social context websites (automated generation of privacy policy),” in *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*. New York, NY: Institute of Electrical and Electronics Engineers, 2017, pp. 1–5.
- [63] S. Yang, Y. Wang, Y. Yao, H. Wang, Y. F. Ye, and X. Xiao, “Describectx: Context-aware description synthesis for sensitive behaviors in mobile apps,” in *2022 IEEE/ACM 44th International Conference on Software Engineering (ICSE)*. New York, NY: Institute of Electrical and Electronics Engineers, 2022, pp. 685–697.
- [64] G. Li, Y. Zhang, X. Yu, and Y. Sun, “ipri: Context-aware access control and privacy policy recommendation,” in *2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom)*. New York, NY: Institute of Electrical and Electronics Engineers, 2015, pp. 370–370.
- [65] P. G. Kelley, L. Cesca, J. Bresee, and L. F. Cranor, “Standardizing privacy notices: an online study of the nutrition label approach,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’10. New York, NY, USA: ACM, 2010, p. 1573–1582. [Online]. Available: <https://doi.org/10.1145/1753326.1753561>

- [66] N. Ebert, K. Alexander Ackermann, and B. Scheppler, “Bolder is better: Raising user awareness through salient and concise privacy notices,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’21. New York, NY, USA: ACM, 2021. [Online]. Available: <https://doi.org/10.1145/3411764.3445516>
- [67] B. Al Muhander, J. Wiese, O. Rana, and C. Perera, “Interactive privacy management: Toward enhancing privacy awareness and control in the internet of things,” *ACM Trans. Internet Things*, vol. 4, no. 3, sep 2023. [Online]. Available: <https://doi.org/10.1145/3600096>
- [68] Y. Feng, Y. Yao, and N. Sadeh, “A design space for privacy choices: Towards meaningful privacy control in the internet of things,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’21. New York, NY, USA: ACM, 2021.
- [69] S. Zhang, Y. Feng, Y. Yao, L. F. Cranor, and N. Sadeh, “How usable are ios app privacy labels?” *Proc. Priv. Enhancing Technol.*, vol. 2022, no. 4, pp. 204–228, 2022. [Online]. Available: <https://doi.org/10.56553/popets-2022-0106>
- [70] I. Ajzen, “From intentions to actions: A theory of planned behavior,” in *Action Control: From Cognition to Behavior*, J. Kuhl and J. Beckmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39. [Online]. Available: https://doi.org/10.1007/978-3-642-69746-3_2
- [71] L. Festinger, “A theory of social comparison processes,” *Human Relations*, vol. 7, no. 2, pp. 117–140, 1954.
- [72] C.-D. Ham, “Exploring how consumers cope with online behavioral advertising,” *International Journal of Advertising*, vol. 36, no. 4, pp. 632–658, 2017. [Online]. Available: <https://doi.org/10.1080/02650487.2016.1239878>
- [73] D. Wilkinson and B. Knijnenburg, “Many islands, many problems: An empirical examination of online safety behaviors in the caribbean,” in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’22. New York, NY, USA: ACM, 2022. [Online]. Available: <https://doi.org/10.1145/3491102.3517643>
- [74] C. Posey, T. Roberts, P. B. Lowry, J. Courtney, and B. Bennett, “Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations,” in *The Dewald Roode Workshop in Information Systems Security 2011*. Blacksburg, Virginia, USA: Social

- Science Research Network, September 22–23 2011, pp. 1–51. [Online]. Available: <https://ssrn.com/abstract=2273594>
- [75] T. Sommestad, H. Karlzén, and J. Hallberg, “A meta-analysis of studies on protection motivation theory and information security behaviour,” *Int. J. Inf. Sec. Priv.*, vol. 9, no. 1, p. 26–46, jan 2015. [Online]. Available: <https://doi.org/10.4018/IJISP.2015010102>
- [76] Y. Feng and Q. Xie, “Privacy concerns, perceived intrusiveness, and privacy controls: An analysis of virtual try-on apps,” *Journal of Interactive Advertising*, vol. 19, no. 1, pp. 43–57, 2019. [Online]. Available: <https://doi.org/10.1080/15252019.2018.1521317>
- [77] Y. Albayram, M. M. H. Khan, T. Jensen, and N. Nguyen, ““...better to use a lock screen than to worry about saving a few seconds of time”: Effect of fear appeal in the context of smartphone locking behavior,” in *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*, ser. SOUPS ’17. USA: USENIX Association, 2017, p. 49–63. [Online]. Available: <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/albayram>
- [78] E. A. Qahtani, M. Shehab, and A. Aljohani, “The effectiveness of fear appeals in increasing smartphone locking behavior among saudi arabians,” in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 31–46. [Online]. Available: <https://www.usenix.org/conference/soups2018/presentation/qahtani>
- [79] C. L. Anderson and R. Agarwal, “Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions,” *MIS Q.*, vol. 34, no. 3, p. 613–643, sep 2010.
- [80] P. Ifinedo, “Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory,” *Comput. Secur.*, vol. 31, no. 1, p. 83–95, feb 2012. [Online]. Available: <https://doi.org/10.1016/j.cose.2011.10.007>
- [81] A. Vance, D. Eargle, K. Ouimet, and D. Straub, “Enhancing password security through interactive fear appeals: A web-based field experiment,” in *2013 46th Hawaii International Conference on System Sciences*. New York, NY: Institute of Electrical and Electronics Engineers, 2013, pp. 2988–2997.

- [82] J. G. P. Jeffrey L. Jenkins, Mark Grimes and P. B. Lowry, “Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals,” *Information Technology for Development*, vol. 20, no. 2, pp. 196–213, 2014. [Online]. Available: <https://doi.org/10.1080/02681102.2013.814040>
- [83] P. Story, D. Smullen, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub, “From intent to action: Nudging users towards secure mobile payments,” in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. Berkeley, CA: USENIX Association, Aug. 2020, pp. 379–415. [Online]. Available: <https://www.usenix.org/conference/soups2020/presentation/story>
- [84] P. Story, D. Smullen, R. Chen, Y. Yao, A. Acquisti, L. Cranor, N. Sadeh, and F. Schaub, “Increasing adoption of tor browser using informational and planning nudges,” *Proceedings on Privacy Enhancing Technologies*, vol. 2022, pp. 152–183, 04 2022.
- [85] A. Chennamaneni and B. Gupta, “The privacy protection behaviours of the mobile app users: exploring the role of neuroticism and protection motivation theory,” *Behaviour & Information Technology*, vol. 0, no. 0, pp. 1–19, 2022. [Online]. Available: <https://doi.org/10.1080/0144929X.2022.2106307>
- [86] A. Ganesh, C. Ndulue, and R. Orji, “Smartphone security and privacy – a gamified persuasive approach with protection motivation theory,” in *Persuasive Technology: 17th International Conference, PERSUASIVE 2022, Virtual Event, March 29–31, 2022, Proceedings*. Berlin, Heidelberg: Springer-Verlag, 2022, p. 89–100. [Online]. Available: https://doi.org/10.1007/978-3-030-98438-0_7
- [87] S. Yin, X. Cai, Z. Wang, Y. Zhang, S. Luo, and J. Ma, “Impact of gamification elements on user satisfaction in health and fitness applications: A comprehensive approach based on the kano model,” *Computers in Human Behavior*, vol. 128, p. 107106, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0747563221004295>
- [88] L. Velykoivanenko, K. S. Niksirat, N. Zufferey, M. Humbert, K. Huguenin, and M. Cherubini, “Are those steps worth your privacy? fitness-tracker users’ perceptions of privacy and utility,” *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 5, no. 4, dec 2022. [Online]. Available: <https://doi.org/10.1145/3494960>
- [89] K. Dhondt, V. Le Pochat, A. Voulimeneas, W. Joosen, and S. Volckaert, “A run a day won’t keep the hacker away: Inference attacks on endpoint privacy zones in fitness tracking social networks,” in *Proceedings of the 2022 ACM SIGSAC Conference on*

- Computer and Communications Security*, ser. CCS '22. New York, NY, USA: ACM, 2022, p. 801–814. [Online]. Available: <https://doi.org/10.1145/3548606.3560616>
- [90] S. Zhang and N. Sadeh, “Do privacy labels answer users’ privacy questions?” in *Workshop on Usable Security and Privacy (USEC 2023)*. San Diego, CA: Network and Distributed System Security (NDSS) Symposium, 01 2023.
 - [91] C. M. K. Cheung and D. R. Thadani, “The impact of electronic word-of-mouth communication: A literature analysis and integrative model,” *Decis. Support Syst.*, vol. 54, no. 1, p. 461–470, dec 2012. [Online]. Available: <https://doi.org/10.1016/j.dss.2012.06.008>
 - [92] M. Vaismoradi, H. Turunen, and T. Bondas, “Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study,” *Nursing & Health Sciences*, vol. 15, no. 3, pp. 398–405, 2013.
 - [93] J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, “The effect of online privacy information on purchasing behavior: An experimental study,” *Information Systems Research*, vol. 22, no. 2, pp. 254–268, 2011. [Online]. Available: <http://www.jstor.org/stable/23015560>
 - [94] H. Habib, Y. Zou, Y. Yao, A. Acquisti, L. Cranor, J. Reidenberg, N. Sadeh, and F. Schaub, “Toggles, dollar signs, and triangles: How to (in)effectively convey privacy choices with icons and link texts,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: ACM, 2021. [Online]. Available: <https://doi.org/10.1145/3411764.3445387>
 - [95] H. Harkous, K. Fawaz, R. Lebet, F. Schaub, K. G. Shin, and K. Aberer, “Polisis: Automated analysis and presentation of privacy policies using deep learning,” in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 531–548. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity18/presentation/harkous>
 - [96] L. F. Cranor, P. Guduru, and M. Arjula, “User interfaces for privacy agents,” *ACM Trans. Comput.-Hum. Interact.*, vol. 13, no. 2, p. 135–178, jun 2006. [Online]. Available: <https://doi.org/10.1145/1165734.1165735>
 - [97] S. Zimmeck, Z. Wang, L. Zou, R. Iyengar, B. Liu, F. Schaub, S. Wilson, N. Sadeh, S. Bellovin, and J. Reidenberg, “Automated analysis of privacy requirements for mobile apps,” in *2016 AAAI Fall Symposium Series*. San Diego, CA: Network

- and Distributed System Security (NDSS) Symposium, 2016. [Online]. Available: <http://dx.doi.org/10.14722/ndss.2017.23034>
- [98] A. Ravichander, A. W. Black, S. Wilson, T. Norton, and N. Sadeh, “Question answering for privacy policies: Combining computational and legal perspectives,” in *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*, K. Inui, J. Jiang, V. Ng, and X. Wan, Eds. Hong Kong, China: Association for Computational Linguistics, Nov. 2019, pp. 4947–4958. [Online]. Available: <https://aclanthology.org/D19-1500>
- [99] T. Li, K. Reiman, Y. Agarwal, L. F. Cranor, and J. I. Hong, “Understanding challenges for developers to create accurate privacy nutrition labels,” in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’22. New York, NY, USA: ACM, 2022. [Online]. Available: <https://doi.org/10.1145/3491102.3502012>
- [100] B. Liu, M. S. Andersen, F. Schaub, H. Almuhiemedi, S. A. Zhang, N. Sadeh, Y. Agarwal, and A. Acquisti, “Follow my recommendations: A personalized privacy assistant for mobile app permissions,” in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 27–41. [Online]. Available: <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/liu>
- [101] D. Smullen, Y. Feng, S. Zhang, and N. Sadeh, “The best of both worlds: Mitigating trade-offs between accuracy and user burden in capturing mobile app privacy preferences,” *Proceedings on Privacy Enhancing Technologies*, vol. 2020, pp. 195–215, 01 2020.
- [102] M. Windl, N. Henze, A. Schmidt, and S. S. Feger, “Automating contextual privacy policies: Design and evaluation of a production tool for digital consumer privacy awareness,” in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’22. New York, NY, USA: ACM, 2022. [Online]. Available: <https://doi.org/10.1145/3491102.3517688>
- [103] R. Ghaiumy Anaraky, Y. Li, and B. Knijnenburg, “Difficulties of measuring culture in privacy studies,” *Proc. ACM Hum.-Comput. Interact.*, vol. 5, no. CSCW2, oct 2021. [Online]. Available: <https://doi.org/10.1145/3479522>
- [104] E. H. R. R. Yao Li and A. Kobsa, “Cultural differences in the effects of contextual factors and privacy concerns on users’ privacy decision on social networking sites,”

- Behaviour & Information Technology*, vol. 41, no. 3, pp. 655–677, 2022. [Online]. Available: <https://doi.org/10.1080/0144929X.2020.1831608>
- [105] P. J. Reed, E. S. Spiro, and C. T. Butts, “Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures,” *Social Science Research*, vol. 59, pp. 155–170, 2016, special issue on Big Data in the Social Sciences. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0049089X16302368>
- [106] S. J. K. Steven Bellman, Eric J. Johnson and G. L. Lohse, “International differences in information privacy concerns: A global survey of consumers,” *The Information Society*, vol. 20, no. 5, pp. 313–324, 2004. [Online]. Available: <https://doi.org/10.1080/01972240490507956>
- [107] S. Cockcroft and S. Rekker, “The relationship between culture and information privacy policy,” *Electronic Markets*, vol. 26, pp. 55–72, 2016.
- [108] D. Das, C. Østerlund, and B. Semaan, “"jol" or "pani"?: How does governance shape a platform’s identity?” *Proc. ACM Hum.-Comput. Interact.*, vol. 5, no. CSCW2, oct 2021. [Online]. Available: <https://doi.org/10.1145/3479860>