

A Tale of Two Communities: Privacy of Third Party App Users in Crowdsourcing - The Case of Receipt Transcription

WEIPING PEI, Colorado School of Mines, USA and The University of Tulsa, USA

YANINA LIKHTENSHTeyn, Colorado School of Mines, USA

CHUAN YUE, Colorado School of Mines, USA

Mobile and web apps are increasingly relying on the data generated or provided by users such as from their uploaded documents and images. Unfortunately, those apps may raise significant user privacy concerns. Specifically, to train or adapt their models for accurately processing huge amounts of data continuously collected from millions of app users, app or service providers have widely adopted the approach of crowdsourcing for recruiting crowd workers to manually annotate or transcribe the sampled ever-changing user data. However, when users' data are uploaded through apps and then become widely accessible to hundreds of thousands of anonymous crowd workers, many human-in-the-loop related privacy questions arise concerning both the app user community and the crowd worker community. In this paper, we propose to investigate the privacy risks brought by this significant trend of large-scale crowd-powered processing of app users' data generated in their daily activities. We consider the representative case of receipt scanning apps that have millions of users, and focus on the corresponding receipt transcription tasks that appear popularly on crowdsourcing platforms. We design and conduct an app user survey study (n=108) to explore how app users perceive privacy in the context of using receipt scanning apps. We also design and conduct a crowd worker survey study (n=102) to explore crowd workers' experiences on receipt and other types of transcription tasks as well as their attitudes towards such tasks. Overall, we found that most app users and crowd workers expressed strong concerns about the potential privacy risks to receipt owners, and they also had a very high level of agreement with the need for protecting receipt owners' privacy. Our work provides insights on app users' potential privacy risks in crowdsourcing, and highlights the need and challenges for protecting third party users' privacy on crowdsourcing platforms. We have responsibly disclosed our findings to the related crowdsourcing platform and app providers.

CCS Concepts: • **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → **Empirical studies in collaborative and social computing**.

Additional Key Words and Phrases: Privacy; App User; Crowdsourcing; Receipt Transcription

ACM Reference Format:

Weiping Pei, Yanina Likhtenshteyn, and Chuan Yue. 2023. A Tale of Two Communities: Privacy of Third Party App Users in Crowdsourcing - The Case of Receipt Transcription. *Proc. ACM Hum.-Comput. Interact.* 7, CSCW2, Article 253 (October 2023), 43 pages. <https://doi.org/10.1145/3610044>

1 INTRODUCTION

In the era of big data, many advanced applications (e.g., mobile and web apps) are data-driven, and they often heavily rely on the data generated or provided by users such as from their uploaded

Authors' addresses: Weiping Pei, Colorado School of Mines, Golden, Colorado, USA, weipingpei@mines.edu and The University of Tulsa, Tulsa, Oklahoma, USA, weiping-pe@utulsa.edu; Yanina Likhtenshteyn, Colorado School of Mines, Golden, Colorado, USA, ylikhten@mines.edu; Chuan Yue, Colorado School of Mines, Golden, Colorado, USA, chuanyue@mines.edu.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

© 2023 Copyright held by the owner/author(s). Publication rights licensed to ACM.

2573-0142/2023/10-ART253 \$15.00

<https://doi.org/10.1145/3610044>

documents and images. For example, face recognition mobile apps need to collect users' facial images on a large scale to train powerful machine learning models [5]. Services provided by those apps assist users in their daily lives and make the world more intelligent.

1.1 Two Communities, Receipt Transcription Tasks, and Knowledge Gap

Unfortunately, those apps may raise significant user privacy concerns. Specifically, to train or adapt their models for accurately processing huge amounts of data continuously collected from millions of app users (as exemplified in Section 2.1), app or service providers have widely adopted the approach of crowdsourcing for recruiting crowd workers to manually annotate or transcribe the sampled ever-changing user data. Robinson et al. found in their 2019 study that “there are at least 250,000 MTurk [Amazon Mechanical Turk, a major crowdsourcing platform] workers worldwide” [56], and note that MTurk is just one of many crowdsourcing platforms [49]. However, when users' documents or images are uploaded through apps and then become widely accessible to hundreds of thousands of anonymous crowd workers (at least on MTurk [56]), many human-in-the-loop related privacy questions arise concerning both the *app user community* and the *crowd worker community*.

Regarding the app user community, questions can be related to app users' privacy awareness, concerns, and potential expectations or needs. For example, if app users are unaware of the public access of their data on crowdsourcing platforms, they need to be explicitly informed of this situation and the potential privacy risks; if app users have concerns on sharing their data with other anonymous individuals, app providers and crowdsourcing platforms should actively take measures to protect app users' privacy. Regarding the crowd worker community, questions can be related to crowd workers' feeling about accessing third party app users' data, their experiences, and their attitudes about potential privacy problems. Note that on crowdsourcing platforms, we refer to task or job requesters as the first party, crowd workers as the second party, and other people (such as app users) whose data would be accessed in a task as *the third party*.

In this paper, we propose to investigate the privacy risks brought by the significant trend of large-scale crowd-powered processing of app users' data generated in their daily activities. In other words, we investigate *the privacy threat from anonymous crowd workers to third party app users*. We consider the representative case of receipt scanning (RS) apps that have millions of users, and focus on the corresponding receipt transcription tasks that appear popularly on crowdsourcing platforms (e.g., they account for 15.1% of available tasks on MTurk according to our observation as described in Section 3.1.2). Receipt images are considered as an important source of private visual information [27, 29]. Privacy concerns on e-receipts related to General Data Protection Regulation (GDPR) [24] and California Consumer Privacy Act (CCPA) [8] exactly reflect the risks of widespread collection, aggregation, and dissemination of personal information by marketers and data brokers [15, 54]. In terms of physical or paper receipts, RS app providers can be directly considered as data brokers [8], while crowdsourcing platforms can be considered as implicit data brokers due to their transactions with the requesters of receipt transcription tasks.

Based on our observations (Section 3.1.2), at least thousands of new receipt images from many countries such as the USA and many types of stores such as pharmacies are posted on MTurk every day; transcribing the sensitive information on them by anonymous crowd workers can infringe on receipt owners' privacy. For example, transcribing medicine items and names or membership IDs on receipts can infringe on receipt owners' health information privacy; transcribing addresses and names or membership IDs on receipts can infringe on receipt owners' geolocation data privacy. Privacy concerns on receipt transcription tasks have been raised in online forums too. For example, an MTurk worker, who is also a co-administrator of the MTurk Crowd forum, wrote on Twitter that “I wonder if Expensify SmartScan users know MTurk workers enter their receipts. I'm looking at

someone's Uber receipt with their full name, pick up, and drop off addresses" [19]. Similar privacy concerns have been raised on other types of transcription tasks such as on transcribing audio [64] and video [50] recordings. As a representative GDPR-related example in industry in 2019, German regulators successfully commanded Google to stop using human contractors to transcribe the voice recordings (for speech recognition improvement purposes) captured by its voice AI services [26].

Unfortunately, as far as we know, no prior studies have formally investigated the privacy risks in either receipt or other types of transcription tasks posted on crowdsourcing platforms. Moreover, crowdsourcing platforms can be considered as one type of human-in-the-loop systems, which are booming in recent years [9, 32, 64, 68, 69]. However, existing studies that have considered the privacy risks in human-in-the-loop systems are largely related to various text, audio, and video based intelligent digital assistants, and their considerations are limited to the specific digital assistant systems or services as reviewed in Section 2.2. Our work not only directly addresses the gap in understanding the privacy risks in realistic receipt transcription tasks that are popularly performed by crowd workers on open platforms, but also broadly contributes to the understanding of the privacy protection challenges that human-in-the-loop approaches have to deal with.

1.2 Two Survey Studies, Research Questions, and Contributions

We first design and conduct an *app user study*. In this first survey study, we recruit mobile app users who have experience in using some RS apps (referred to as **RS app users**) to understand how they perceive privacy while using those apps; we also recruit mobile app users who have not used any RS app yet (referred to as **NRS app users**) to understand how general app users would consider the information on receipts and the potential use of RS apps. Specifically, we aim to solicit the responses from both RS and NRS app users to answer the following two research questions:

RQ1: What is app users' understanding of the data extraction and sharing practices of RS apps? In more details, where do app users think the information on the scanned receipts is extracted (RQ1-1)? To whom do app users think the information on the scanned receipts will be shared (RQ1-2)? Do RS and NRS app users differ in their responses to these questions (RQ1-3)? Answering these questions will help us gauge app users' understanding of possible access to their receipts by others.

RQ2: How do app users feel about having their receipts accessible to anonymous individuals? In more details, how comfortable would app users feel about having their receipts with different types of information accessible to anonymous individuals (RQ2-1)? What are app users' opinions on protecting the information on receipts (RQ2-2)? Do RS and NRS app users differ in their responses to these questions (RQ2-3)? With these questions being answered, better guidelines could be developed to help reduce app users' potential privacy risks.

On the other hand, we design and conduct a *crowd worker study*. In this second survey study, we recruit crowd workers who are able to access and perform receipt transcription tasks on MTurk to understand their experiences on receipt and other types of transcription tasks as well as their attitudes towards such tasks. Specifically, we aim to solicit the responses from crowd workers to answer the following two research questions:

RQ3: What are crowd workers' opinions about the sensitivity of the information on receipts and their experiences with receipt transcription tasks? In more details, what information on receipts is considered as sensitive by crowd workers (RQ3-1)? What are crowd workers' experiences on transcribing receipts that contain sensitive information (RQ3-2)? What are crowd workers' experiences on transcribing other documents that contain sensitive information (RQ3-3)? Answering these questions will provide more insights about crowd workers' opinions and experiences on transcription tasks.

RQ4: What are crowd workers' attitudes towards privacy problems in receipt transcription tasks? In more details, what are crowd workers' opinions on protecting the information on receipts (RQ4-1)? How do they feel about working on receipt transcription tasks that contain app users' sensitive information (RQ4-2)? Do they have similar feelings towards having their own receipts transcribed by other workers (RQ4-3)? What is crowd workers' understanding of the receipt transcription task requesters and their purposes (RQ4-4)? Exploring the answers to these questions will help us assess the privacy risks of disclosing app users' sensitive information to the crowd worker community, and identify appropriate privacy protection solutions.

To answer RQ1 and RQ2, we recruited 56 RS and 52 NRS app users from the Reddit and Craigslist communities (Section 3.2.3) to participate in our app user study. Our analysis shows that there is a higher percentage of RS app users than NRS app users who believed that the information on receipts will be extracted within an app itself and their receipts will not be accessible by other parties and anonymous individuals. Meanwhile, 80.4% of RS and 92.3% of NRS app users had strong concerns about having their sensitive information on receipts accessible by anonymous individuals. To answer RQ3 and RQ4, we recruited 102 crowd workers from MTurk (Section 3.3.2) to participate in our crowd worker study. In general, crowd workers considered that the information of customers (i.e., receipt owners) is more sensitive than that of vendors (i.e., stores), and 44.1% of them reported working on receipt transcription tasks that contain sensitive information at least monthly. Only 43.1% of crowd workers expressed being comfortable with working on receipt transcription tasks that contain the information of customers, while only 11.8% of crowd workers were comfortable with having their own receipts that contain sensitive information transcribed by other crowd workers. From these two studies, over 96.4% of app users and 99.0% of crowd workers agreed or strongly agreed with the importance of protecting the privacy of customers on receipts.

To summarize, we make three major contributions in this paper: (1) we propose to investigate the privacy risks of third party app users in crowdsourcing, and to answer a number of human-in-the-loop related privacy questions concerning both the app user community and the crowd worker community; (2) we identify RS apps and the corresponding receipt transcription tasks as a representative case to investigate the privacy risks brought by the significant trend of large-scale crowd-powered processing of app users' data; (3) we design and conduct two complementary user studies, and derive insights on the need and challenges for protecting third party users' privacy on crowdsourcing platforms.

The rest of this paper is organized as follows. Section 2 introduces the background and related work. Section 3 describes the design of the two survey studies. Section 4 presents and analyzes the results of the two studies. Section 5 discusses the implications of our key findings and provides our recommendations to stakeholders; it also discusses the limitations of this work and the potential future work. Section 6 concludes the paper.

2 BACKGROUND AND RELATED WORK

In this section, we introduce the background of receipt scanning (**RS**) apps and review privacy related studies.

2.1 Background

In recent years, continuously collecting and processing users' data has become an important trend in mobile apps. One representative example is the surge of the receipt scanning apps. There are hundreds of RS apps on Google Play and Apple App stores, and they have attracted millions of users to upload the receipts from their daily lives. For example, as shown in Table 5 in Appendix C.1, 10 out of 14 popular RS apps have millions of downloads on the Google Play store. RS apps can be categorized into two types: **rewards apps** that offer users rewards such as cashback on

certain expenses, and **finance apps** that provide users with services such as expense or receipt management. Besides some individual developers, the providers of RS apps are mainly companies such as Expensify and Ibotta. It is unclear to us how exactly users' receipts contribute to the business models of RS app providers. However, most RS apps transfer users' receipts to remote servers, and most of them indicated in their privacy policies the possibility of sharing the collected data to third parties as shown in our analysis of 14 popular RS apps (Section 5.1). Although it also remains unclear to us whether partial or all receipts collected by RS apps are manually transcribed (more discussion is in Section 5.2), receipt transcription tasks are very popular in crowdsourcing, for example, they account for 15.1% of available tasks on MTurk according to our observation as described in Section 3.1.2.

Besides the efforts from companies and individual developers, many researchers also work actively on improving or designing new RS apps. For example, Sainz-De-Abajo et al. developed an app for the elderly to control their diet by scanning grocery receipts [58]. Some researchers focus on designing new methods to more accurately extract the information on receipts. For example, Zhu et al. proposed using optical character recognition (OCR) to digitize receipts with the help of conditional random fields and regular expressions [70]. Since OCR results are error-prone and they heavily depend on the quality of images [17], more advanced approaches have been proposed. For example, Altmeyer et al. presented a crowd-based approach that leverages crowdsourcing to improve the outcome of OCR for an expense control app [4]. However, none of these studies considered the potential privacy risks that could be incurred to the users of RS apps.

2.2 Related Work

Receipt transcription tasks are very popular in crowdsourcing as we just introduced, but we could not find prior studies that have formally investigated the privacy risks in either receipt or other types of transcription tasks posted on crowdsourcing platforms. We now review three main categories of privacy related studies and summarize the knowledge gap that our work contributes to address.

Privacy of mobile app users. App users' privacy has been intensively studied over the years as mobile apps can often access many types of sensitive data of users. Some researchers focused on exploring users' expectations, concerns, and behaviors around privacy when using mobile apps; they found that app users are often unaware of the collection of their sensitive data and often express concern or discomfort when they learn about it [21–23, 44, 61]. Some other researchers focused on proposing technical solutions to protect app users against privacy leakage [2, 28, 45, 55]. Investigating privacy attacks such as tracking smartphone users via browser, app, or device fingerprinting and the corresponding defenses represents another line of research [12–14, 16, 30, 42, 62]. However, all these studies are not about the privacy issues of having app users' data accessible on crowdsourcing platforms.

Privacy risks to crowd workers. With the booming of crowdsourcing in recent years especially for annotating various datasets of AI systems by recruiting a large number of anonymous workers, privacy risks in crowdsourcing are increasingly attracting researchers' attention. Prior studies mainly focused on exploring and understanding the privacy risks to crowd workers, such as how they can be de-anonymized and their information can be disclosed [33, 35, 40]. For example, Xia et al. surveyed MTurk workers to understand their privacy concerns, experiences of privacy loss, and privacy expectations [65]. They found that sensitive information (e.g., identity and financial information) inquiry and email address collection (for ads or spamming) are two major privacy issues reported by the respondents from multiple countries and areas. Sannon et al. interviewed MTurk workers to understand how they navigate the risks of being asked to provide their personal information in tasks [60]. They found that workers may avoid risky tasks, tell "privacy lies", or provide only partial information to protect their privacy, and may also report risky tasks to the

MTurk platform. However, as more mobile apps have their users' data processed on crowdsourcing platforms, little is known regarding how app users would consider the potential privacy risks to them and how crowd workers would perceive such privacy risks.

Privacy in the human-in-the-loop digital assistant systems. Crowdsourcing platforms can be considered as one type of human-in-the-loop systems. Existing studies that have considered the privacy risks in human-in-the-loop systems are largely related to various text, audio, and video based intelligent digital assistants such as in [10, 31, 63]. Their considerations can, to a good extent, be attributed to the warnings from some early studies on the viability of information extraction threats in crowd-powered systems. For example, Lasecki et al. showed that a sizable portion of MTurk workers were willing to extract information from fake credit card pictures, and warned that malicious workers may begin performing such information extraction attacks [39].

In more details, Jahanbakhsh et al. built a human-in-the-loop Q&A system which leverages knowledgeable workers to supervise or complement document-centered AI assistants to better answer users' complex questions [31]. They briefly discussed that privacy will be a challenge if the documents are confidential and workers are externally recruited. Cranshaw et al. designed a three-tiered Calendar.help architecture which provides fast and efficient meeting scheduling through structured workflows with the collaboration of AI-powered agents and human workers of varying expertise [10]. They required the workers in their study to sign a non-disclosure agreement to ensure confidentiality; however, they suggested that future crowd-powered tasks should intentionally anonymize users' data for privacy protection like what Kaur et al. did in segmenting images into small pieces so that an individual worker can only have the access to the partial information in any image [34]. Swaminathan et al. designed the WearMail conversational interface to assist users in retrieving specific information in their emails via a privacy-preserving human computation workflow [63]. They allowed crowd workers to only interact with the heavily-obfuscated email meta-data for generating filters which are used to automatically extract the desired information in emails.

Summary of knowledge gap and our contribution. The intelligent digital assistants reviewed above are specific systems or services, and they directly collect or provide the data to be processed by humans. However, we are concerned about the privacy risks brought by the significant trend of large-scale crowd-powered processing of millions of app users' data generated in their daily activities such as shopping. Our work not only directly addresses the gap in understanding the privacy risks in realistic receipt transcription tasks that are popularly performed by crowd workers on open platforms, but also broadly contributes to the understanding of the privacy protection challenges that human-in-the-loop approaches have to deal with.

3 DESIGN OF THE TWO SURVEY STUDIES

Researchers typically take either the survey approach (e.g., in [23, 44, 65]) or the semi-structured interview approach (e.g., in [38, 60]) in conducting privacy related user studies. In some studies such as [21, 61], both approaches are taken. Survey studies can be both quantitative and qualitative, while semi-structured interview studies are largely qualitative. We take the survey approach and design two survey studies with both open-ended and close-ended questions; this will allow us to conveniently perform between-subjects as well as within-subjects comparisons, and to both quantitatively and qualitatively answer our four research questions. Before detailing the design of our two survey studies, we describe some important considerations that influenced our design.

3.1 Important Design Considerations

3.1.1 The Connection between the Two Communities. Figure 1 illustrates the connection between the app user community and the crowd worker community. After completing the transactions with

vendors, app users scan (i.e., take the photos of) their receipts using RS apps, which all have an in-app camera function and often automatically upload the receipt images to the app providers' remote servers (Section 5.1). Task requesters who are partnered with the app providers or data brokers obtain the receipts and upload them to crowdsourcing platforms in receipt transcription tasks. Anonymous workers can then transcribe or simply view the receipt images.

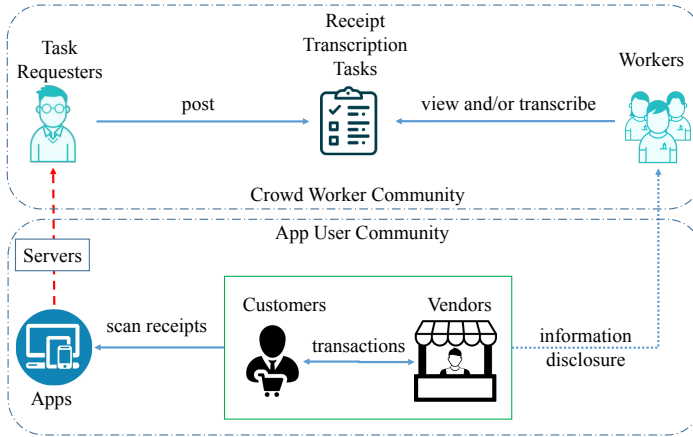


Fig. 1. The Connection between the Two Communities.

Although we could not identify official reports or existing studies that document the connection between the crowd worker community and the app user community, we found two types of indications pertaining to this connection by using the lookup method which is “the most basic kind of search task” [47] that everyone can easily try and verify its results.

First, using any MTurk worker account, one can notice that at least thousands of unique receipt images are posted in various receipt transcription tasks every day. Previewing randomly-sampled receipt images, one can see that majority of receipts are very fresh (within hours or days of transactions between customers and stores) and diverse (from many countries such as the USA, UK, and Netherlands, and from many types of stores such as supermarkets, pharmacies, and gas stations). One can notice that the backgrounds of receipt images are also very diverse, e.g., in cars, rooms, and outdoor environments with different angles and light conditions. In addition, viewing the metadata of receipt images, one can see that many receipt images retained very diverse camera make, camera model, and GPS information. All these indicate that receipt photos on MTurk were largely taken by their owners using smartphones.

Second, searching “receipt scanner” on Google Play and Apple App stores, one can easily find hundreds of RS apps and notice some correlations between popular RS apps and major requesters who have continuously launched receipt transcription tasks on MTurk. One example is the “Ibotta” app and the requester named “Ibotta, Inc” (lately changed the name to “Receipt Processing”). Another example is the “GetUpside” app developed by the Upside Services, Inc and the requester named “Upside Services Inc”. These correlations indicate the connection between the two communities.

These two types of indications led to and justified the most important early design decision for our work, that is, designing two *independent but correlated* (especially in terms of some questions) survey studies to collectively answer our four research questions. One additional note is that correspondingly in our crowd worker study, we designed questions to solicit opinions from crowd workers regarding how task requesters obtained the receipts. Later at the end of Section 4.2.3, we

can see that many crowd workers considered RS apps as the major source of the receipt images on MTurk, which further confirms the connection between the two communities.

3.1.2 Types of Information and Their Sensitivity. Exploring the types of information that can be extracted from receipt images will not only help assess risks of disclosing app users' receipts to the crowd worker community, but also help design our two survey studies in terms of some common questions. Our exploration is based on the manual previewing (without taking and interfering with the tasks) of receipt transcription tasks on MTurk with the IRB approval and careful ethical considerations (Section 3.5). It follows the observational measurement of behavior methodology [66], but is lightweight with the focus on task requesters' behaviors in naturalistic contexts.

To present the recent information to readers, we used our MTurk worker account and manually explored the 50 freshest task groups on MTurk three times a day (at 10:00 AM, 2:00 PM, and 8:00 PM in Pacific Time) for two weeks (one is in March and the other is in April of 2022). By checking the task titles and descriptions, we observed that each time an average of 53,911 tasks exist in the 50 groups with 15.1% (8,123) of them being receipt transcription tasks. We previewed (without downloading) 147 randomly-sampled unique receipt images (roughly 10 per day in those two weeks), and wrote the ethnographic notes (for ethical considerations [46], i.e., without extracting or recording the detailed content of any receipt) about the types of information and their sensitivity from two perspectives (visible information on receipts and metadata of receipt images) as follows.

Visible information on receipts. We counted the occurrences of different types of visible information on the 147 receipts as shown in Table 1. We can see that the information could be customer related (e.g., customer's name) or vendor related (e.g., store's name). As expected, we observed a high percentage of receipts containing information of vendors, e.g., 146 (99.3%) receipts contain a store's name. However, a considerable percentage of receipts contain sensitive information of customers (i.e., app users), e.g., 21 (14.3%) receipts contain a customer's name. Customers' names, phone numbers, home addresses, and membership IDs etc. typically are personal identifiable information (PII) and should be protected according to GDPR [24]. Furthermore, combinations of common types of information, e.g., a store's address (85.7%) and a customer's last 4 digits of a credit card (70.1%), could be used to identify customers and associate their activities in different stores in a given region; the date and time information (98.0%) could be helpful too.

Table 1. Information on the 147 Sampled Receipts.

Visible Information Type on Receipts	Occurrence (%)
Customer's Name	21(14.3%)
Customer's Phone Number	1(0.7%)
Customer's Home Address	9(6.1%)
Customer's Last 4 Digits of a Credit Card	103(70.1%)
Customer's Membership ID	58(39.5%)
Store's Name	146(99.3%)
Store's Address	126(85.7%)
Store's Phone Number	92(62.6%)
Store Employee's Name	45(30.6%)
Date and Time of the Transaction	144(98.0%)
Metadata of Receipt Images	Occurrence (%)
Camera Make and Model	38(25.9%)
GPS Information	6(4.1%)

Metadata of receipt images. The Exchangeable Image File Format (EXIF) metadata of receipt images may also reveal information that can be used for locating or identifying app users. To check the metadata of those 147 receipt images, we used the EXIF Viewer Firefox browser extension [18],

which allows us to simply view the metadata without downloading the image files. As shown in Table 1, we found that 38 (25.9%) receipt images contain the camera make and model information, and 6 (4.1%) receipt images contain the exact GPS information of the receipt scanning location. It is worth noting that while we did not download receipt images in exploring their visible information and metadata, anyone with a worker account (which can be easily created) including crowd workers and attackers can easily download or record the previewed receipt images for large-scale offline analyses.

Although both visible information on receipts and metadata of images could reveal sensitive information of app users, we only consider the former in the design of our two survey studies as visible information is straightforward to both app users and crowd workers. Because the types of information on receipts can be an important factor that influences participants' responses in both studies, we design survey questions with those information types as the options to explore how participants' responses may vary across them. Specifically, in the app user study, we design a question for app users to indicate their comfort levels with disclosing different types of information on receipts. In the crowd worker study, we design one question for crowd workers to select the sensitive types of information, and another question for them to select the types of information they have ever seen in receipt transcription tasks.

3.2 Design of the App User Study

To answer RQ1 and RQ2, we design the app user study. We first ask participants to take a screening survey (Appendix A.3) to determine their eligibility (e.g., they must be adults in the USA for compensation) and if they are RS vs. NRS app users. We consider both RS and NRS app users because responses of NRS app users could provide insights into how general app users would consider the information on receipts and the potential use of RS apps. Eligible RS and NRS app users are invited to take the follow-up survey.

3.2.1 Selection of Apps and Usage Scenarios. We searched on the Google Play store for RS apps using the keywords "receipt tracking" and "receipt scanner", compiled a list of 30 most popular RS apps based on the number of downloads, narrowed down the list based on relevance (e.g., removing apps such as local scanners that do not support features for uploading receipts), and selected the 11 most relevant and popular RS apps as the options in the question (AQ1-3 in Appendix A.1) that explores app users' usage of RS apps. Six of them are rewards apps and the other five are finance apps as shown in Table 5 in Appendix C.1. As NRS app users did not have any experience in using RS apps, a usage scenario should be provided to help them understand the procedure of using those apps and answer questions. We design a *Rewards App* scenario and a *Finance App* scenario, and randomly display one of them as the prompt just to each NRS app user before showing the related questions.

3.2.2 Design of the Detailed Survey Questions. The follow-up survey consists of 26 (24 for NRS app users) open-ended and close-ended questions (as shown in Appendix A.1). We use the **AQ** prefix ('A' for app users) to number the questions in this survey, and group them into five sets (AQ1~AQ5). AQ1 questions are about whether a participant has used some RS apps before and how often and long is the usage. AQ2 questions are for RQ1 regarding app users' understanding of data extraction and sharing practices of RS apps. AQ3 questions are about app users' feeling on having their receipts accessible to anonymous individuals. Specifically, we first present a scenario that apps may share users' receipts with anonymous individuals for transcription, and then ask participants about their comfort levels with regard to this scenario. AQ4 questions are about participants' opinions on who should be responsible for keeping sensitive receipt information protected. Analyzing participants' responses to AQ3 and AQ4 will help us answer RQ2. AQ5 questions are about the demographics of

participants. In addition, we insert an attention check question somewhere in the middle of the survey to help filter out low-quality responses provided by participants.

3.2.3 App User Recruitment and Compensation. We leveraged the Reddit communities (e.g., r/SampleSize, r/Ibotta, and r/Quickbooks) and Craigslist communities (e.g., the computer gigs and volunteer sections in 30 cities of the USA) to recruit app user participants. Those who provide high-quality responses to all questions in the screening survey will receive the link of the follow-up survey via email. We described the goal of our study as “understanding users’ opinions regarding mobile apps”, purposefully not mentioning privacy concerns of uploading receipts to avoid priming participants and to limit the self-selection bias.

The formal app user study was conducted in the middle of 2021. It is worth mentioning that we intentionally avoided recruiting app users from any crowdsourcing platform to minimize the potential interference between the app user study and the crowd worker study. The follow-up survey takes participants about 10 minutes to complete. We attracted participants with considerable compensation, with all qualified participants being compensated with a 10 USD Amazon gift card.

3.3 Design of the Crowd Worker Study

To answer RQ3 and RQ4, we design the crowd worker study. Since we need not differentiate crowd workers (unlike that in the app user study for RS vs. NRS app users), there is no screening survey.

3.3.1 Design of the Detailed Survey Questions. The survey in this study consists of 31 open-ended and close-ended questions (as shown in Appendix B.1). We use the **TQ** prefix (“T” for turkers) to number the questions in this survey, and group them into six sets (TQ1~TQ6). We first displayed one of our receipts, and asked crowd workers to answer TQ1 questions which are about identifying all types of information from the given receipt. The purpose of TQ1 is for crowd workers to recall or become familiar with the terms such as customer and vendor. The analysis of TQ1 shows that most of crowd workers can correctly identify all types of information on the receipt. TQ2 questions ask crowd workers to indicate the types of sensitive information on receipts and how often they see tasks with sensitive information. TQ3 questions are about crowd workers’ experiences with transcription tasks on crowdsourcing platforms. The goal of designing TQ2 and TQ3 is to answer RQ3. TQ4 questions are about crowd workers’ attitudes towards privacy risks on MTurk, including their opinions on privacy protection and their comfort levels with working on tasks that contain sensitive information. TQ5 questions are about crowd workers’ opinions on the requesters’ task purposes, identities, and receipt sources. Analyzing participants’ responses to TQ4 and TQ5 will help us answer RQ4. TQ6 questions are about the demographics of participants. An attention check question is also inserted as in the app user study.

3.3.2 Crowd Worker Recruitment and Compensation. We recruited crowd worker participants from MTurk, and the formal crowd worker study was conducted in September 2021. This survey takes crowd workers at most 15 minutes to complete, and all qualified crowd workers were compensated with four USD through MTurk. The projected hourly wage is 16 USD/hr, which is above the required minimum wage of 7.25 USD/hr in the USA.

3.4 Data Analysis Methodology

For close-ended questions, we describe the answer distributions and also perform nonparametric statistical tests for quantitative analysis. To perform between-subjects comparison of ordinal data (e.g., responses on comfort levels), we use the Wilcoxon rank sum test for two groups (e.g., RS app users vs. NRS app users) and the Kruskal-Wallis test for three groups. To perform within-subjects comparison of ordinal data, we use the Wilcoxon signed rank test. Besides, we use the

Chi-square test of independence for inspecting the relationship between two categorical variables. We calculated the required sample sizes for the statistical tests to be performed using a power analysis (as in [3, 43, 48]). With the 95% confidence interval, 80% power, and effect size $d = 0.8$, the required sample size is 52 in each group. Thus, we recruited 52 and 56 valid RS and NRS app users, respectively (Section 4.1.1), and recruited 102 valid crowd workers (Section 4.2.1).

For open-ended questions, we code the responses and quote representative ones for qualitative analysis. Taking the thematic analysis approach [7] and following recent practices (e.g., as in [57, 67]), two coders (the first two authors) were involved in the coding and analysis process. For each open-ended question, the two coders independently coded 20% of responses before discussing and agreeing on an initial version of the codebook. Based on the initial codebook, the two coders independently coded all remaining responses. For the responses that could not be coded into the existing codes of the initial codebook, new codes were introduced and added to the codebook. We then calculated the inter-coder reliability Krippendorff's α coefficient [37, 57, 67] for each open-ended question as shown in Table 6 in Appendix C.2. The average and the standard deviation of all reliability coefficients are 0.86 and 0.07, respectively, indicating a high level of agreement among the two coders. Afterwards, the two coders discussed all codes, consolidated them, and refined them to finalize the codebook. With the final codebook, the two coders independently re-coded all responses to ensure that no information was missed. The final codebook contains 145 codes across 15 code categories as shown in Table 7 and Table 8 in Appendix C.2 for the app user study and the crowd worker study, respectively.

3.5 IRB Approval, Ethical Considerations, and Pilot Study

We received the IRB approval to preview the receipt images in transcription tasks (Section 3.1.2) and to conduct both survey studies. We strictly adhered to the approved IRB protocol to safeguard the privacy and security of both participants and receipt owners. We did not collect any sensitive information from participants, and we securely stored all their responses. We did not download receipt images and did not explicitly extract any specific individuals' sensitive information from receipts - we only statistically counted the occurrences of information types and wrote the ethnographic notes as described in Section 3.1.2.

Before conducting the formal app user and crowd worker studies, we first internally ran a pilot study with our colleagues and students to mainly help us check the correctness of the survey procedure, the clarity of the survey questions, and the survey completion time. We did not observe any major problem, and did not receive any major comment. We only made some minor wording changes to finalize the survey questions described in Sections 3.2.2 and 3.3.1. These internal participants were excluded from the formal studies, and their responses were excluded from the formal result analysis (Section 4). Note that we also had one question at the end of each formal study (Appendix A.1 and Appendix B.1) for collecting additional comments or concerns from participants. Both formal studies went smoothly and we did not receive any major comment or complaint, so we did not make any further changes.

4 RESULTS OF THE TWO STUDIES

We now present and analyze the results of the two studies.

4.1 Results of the App User Study

We first present the demographics and RS app usage statistics of participants. We then detail the results to answer RQ1 and RQ2.

4.1.1 Demographics and App Usage. A total of 247 people took the survey in our app user study. After filtering out participants who answered the attention check question incorrectly, provided inconsistent answers between the screening survey (Appendix A.3) and the follow-up survey (Appendix A.1), or provided completely irrelevant answers to open-ended questions, we were left with 108 valid participants. Note that it is normal to filter out many participants recruited from online communities for quality control purposes [52, 53]. Out of the valid participants, 56 were RS app users who have experience in using some RS apps, and 52 were NRS app users who have not used any RS app yet. Table 3 in Appendix A.2 summarizes the demographics of RS and NRS app users. In brief, 48.2% of RS app users were between 18 and 24 years old, while most (51.9%) of NRS app users were between 25 and 39 years old. As for the gender, 51.8% of RS app users were female, while 44.6% were male and 3.6% were non-binary; NRS app users were evenly split between male and female.

RS app users also reported their app usage time and frequency as shown in Table 3 in Appendix A.2. From their responses to AQ1-3, the four most commonly used apps were Ibotta (67.9%), Receipt Pal (42.9%), Fetch (37.5%), and Receipt Hog (26.8%); all four are rewards apps. As expected, the main reason for using RS apps (AQ1-2) was to obtain monetary benefits (e.g., cashback and gift cards) as indicated by 44 (78.6%) RS app users. Another popular reason was to track the budget with digital copies of receipts as indicated by seven (12.5%) RS app users. As for how long they have been using RS apps, 76.8% of RS app users answered more than or around one year (AQ1-4). Meanwhile, the majority (76.8%) of RS app users reported using RS apps once a week or more frequently (AQ1-5). Most (66.1%) of RS app users did not read the privacy policies of RS apps (AQ1-6).

4.1.2 RQ1: Users' Understanding of Data Extraction and Sharing Practices of RS Apps. Figure 2 summarizes the 108 app users' responses to questions about their understanding of data extraction (Figure 2a) and data sharing (Figure 2b) practices of RS apps. Regarding the question (AQ2-1) if the information on receipts is extracted locally or remotely, more than half of RS app users (58.9%) believed that the information on receipts would be extracted by the app itself locally on the phone, whereas the majority (61.5%) of NRS app users doubted that. The Chi-square test of independence found that there is a statistically significant relationship between the RS app usage and a user's belief on local vs. remote extraction of receipt information. This difference in the perception of data extraction implies that RS app users are less sensitive than NRS app users on the potential access of receipts by remote servers.

As for the question (AQ2-2) if the information is extracted within a RS app or third parties (e.g., other apps, online platforms, and service providers), 66.1% of RS app users somewhat agreed or strongly agreed that "the receipt information is extracted within the app instead of third parties"; only 46.2% of NRS app users somewhat agreed or strongly agreed with the statement. The difference between the answer distributions of RS and NRS app users on AQ2-2 is not statistically significant based on the Wilcoxon rank sum test ($p > 0.05$). This result implies that RS app users have the similar perception with NRS app users in terms of whether third parties would be involved in data processing. In Figure 2a, it is noticeable that a non-negligible percentage (17.3%) of NRS app users strongly disagreed with AQ2-2 while none of RS app users indicated strong disagreement; this result might be related to why those NRS app users did not use RS apps in the first place. On the other hand, it is surprising to see more NRS app users (25.0%) than RS app users (16.1%) strongly agreed with the statement; this result might be related to the possibility that some NRS app users were even unaware of the existence of RS apps before participating in our study.

Overall, the majority of RS app users believed that the receipt information is extracted locally on a phone and within the app, which might lead them to be less thoughtful of their privacy with respect to using RS apps. However, later in Section 5.1 we will show in our analysis of popular RS

apps' network traffic behaviors that most (12 out of 14) apps send receipt images to remote servers for processing, revealing the mismatch between most RS app users' understanding of RS apps' data extraction practices and the reality.

Regarding their understanding of data sharing practices of RS apps, 44.6% of RS app users believed (i.e., somewhat agreed or strongly agreed) that their receipt images will not be shared to other parties (AQ2-3), whereas only 34.6% of NRS app users believed so. The difference between the answer distributions of RS and NRS app users is statistically significant ($p < 0.05$) according to the Wilcoxon rank sum test. In Figure 2b, we can also notice that more NRS app users (36.5%) than RS app users (12.5%) strongly disagreed with AQ2-3, which might be also related to why those NRS app users did not use RS apps in the first place. For the statement that "My receipts will not be shared to some anonymous individuals" (AQ2-4), the level of agreement is increased to 55.4% and 40.4% from RS and NRS app users, respectively. The difference between the answer distributions of RS and NRS app users is also statistically significant ($p < 0.05$) according to the Wilcoxon rank sum test. Similar to that with AQ2-3, noticeably more NRS app users (25.0%) than RS app users (7.1%) strongly disagreed with AQ2-4. Meanwhile, noticeably more RS app users (41.1%) than NRS app users (19.2%) strongly agreed with AQ2-4. The values of Cronbach's alpha [11] for RS ($\alpha=0.83$) and NRS ($\alpha=0.93$) app users are greater than 0.70, indicating satisfactory internal consistencies for this construct of two statements AQ2-3 and AQ2-4.

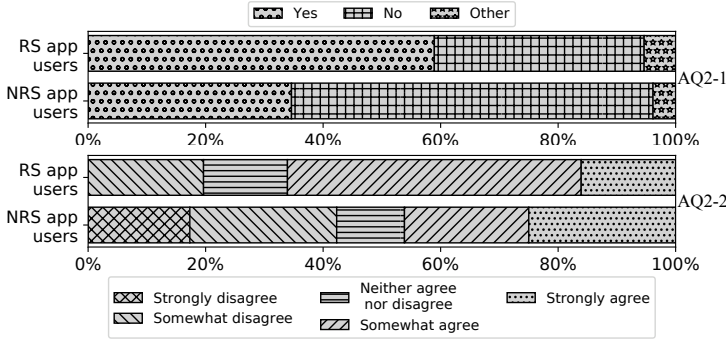
Overall, more RS app users than NRS app users believed that their receipts will not be accessible by other parties and anonymous individuals, indicating that such beliefs of those RS app users might also lead them to be less thoughtful of their privacy with respect to using RS apps. Later in Section 5.1 we will show in our analysis of popular RS apps' privacy policies that most (13 out of 14) apps indicated that they may share the collected data with third parties and two apps indicated the human involvement in data processing, revealing the mismatch between many RS app users' understanding of RS apps' data sharing practices and the reality.

4.1.3 RQ2: App Users' Feeling About Having Their Receipts Accessible to Anonymous Individuals.

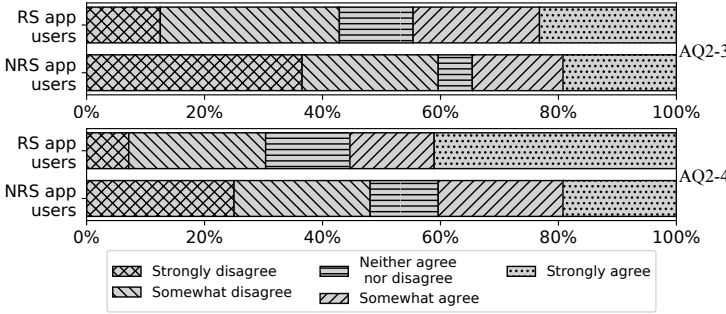
General comfort level or feeling. We first prompted both RS and NRS app users that their receipts could be accessible by other parties or anonymous individuals for data extraction; we then asked them to rate the level of comfort with having their receipts transmitted to other parties and accessed by anonymous individuals on a 5-level Likert scale from very comfortable to very uncomfortable (AQ3-1). As shown in the upper portion of Figure 3, a large percentage (48.2%) of RS app users were uncomfortable or very uncomfortable on AQ3-1, while the corresponding percentage for NRS app users is much higher (65.4%); especially, noticeably more NRS app users (48.1%) than RS app users (12.5%) were very uncomfortable on AQ3-1. The Wilcoxon rank sum test found that this difference between RS and NRS app users is statistically significant ($p < 0.05$), indicating that NRS app users are more concerned than RS app users about the disclosure of their general receipts to other parties or anonymous individuals.

When receipts contain sensitive information of app users (AQ3-3), most RS (80.4%) and NRS (92.3%) app users were uncomfortable or very uncomfortable with having their receipts transmitted to other parties and accessible by anonymous individuals. There is no statistically significant difference between RS and NRS app users on this question according to the Wilcoxon rank sum test ($p > 0.05$), indicating that most of them all have severe concerns about revealing their sensitive information on receipts.

These results from AQ3-1 and AQ3-3 highlight that most app users do have concerns about their privacy pertaining to receipts. They indicate that RS app users' misunderstanding of RS apps' data extraction and sharing practices as analyzed above in Section 4.1.2 is indeed a problem.



(a) Data Extraction. (AQ2-1: Do you believe that the information is extracted by the app itself locally on your phone instead of transmitting receipts to remote servers for information extraction? AQ2-2: I believe that the receipt information is extracted within the app instead of third parties.)



(b) Data Sharing. (AQ2-3: My receipts will not be shared to other parties. AQ2-4: My receipts will not be shared to some anonymous individuals.)

Fig. 2. App Users' Understanding of Data Extraction and Sharing Practices of RS Apps.

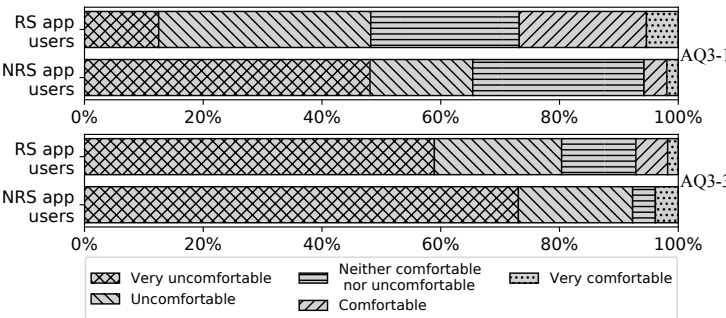


Fig. 3. App Users' Comfort Level for Having Receipts Accessible to Anonymous Individuals. (AQ3-1: How comfortable would you feel if your uploaded receipts are transmitted to a third party and accessed by anonymous individuals? AQ3-3: How comfortable would you feel if a receipt containing your sensitive information is transmitted to a third party and accessed by anonymous individuals?)

Reasons for comfort or discomfort. AQ3-2 and AQ3-4 are open-ended questions that asked app users to explain their answers to AQ3-1 and AQ3-3, respectively.

Among 15 RS app users who selected comfortable or very comfortable for AQ3-1, five considered the information on receipts trivial, e.g., *"They're just receipts, nothing too personal"* (RS app user #26); four stated that the rewards obtained from the apps outweigh potential risks, e.g., *"I know it is happening, and I doubt there is anything I can do to change it. The rewards outweigh the risks in this case"* (RS app user #1); two just would not mind, e.g., *"For me, I would not mind it because the receipts I have is already money spent on things I had to purchased"* (RS app user #32); four had other reasons. We can see that monetary rewards can to some extent alleviate some users' privacy concerns, which is similar to the observation in previous studies [41, 59].

Among 27 RS app users who selected uncomfortable or very uncomfortable for AQ3-1, 15 had concerns on privacy disclosure, e.g., *"Because it doesn't protect my privacy since someone may estimate my income. It may lead to increase in price of goods when a company knows the rate at which goods are bought"* (RS app user #33); nine worried about other potential risks such as identity theft, e.g., *"I think the fact that this data which has my payment methods and such is being transcribed by another person whom I don't know puts me at a risk for identity theft at the very least"* (RS app user #4); two highlighted their concerns on being unclear how the information would be processed and used, e.g., *"I would like to know what they are doing with this information. The unknown is what worries me"* (RS app user #8); the remaining one had other reasons. Although these RS app users provided diverse reasons, most of them were concerned about the negative privacy or security consequences of having other people access their receipts.

As for NRS app users, three selected comfortable or very comfortable for AQ3-1: one considered the information trivial, one just would not care, and one had already adopted privacy protection before submitting receipts; 34 selected uncomfortable or very uncomfortable for AQ3-1 with the reasons similar to those from RS app users: 10 had concerns on privacy disclosure, eight worried about potential risks, three highlighted their concerns on lack of transparency, and 13 simply expressed discomfort in sharing.

We observed that 18 RS and 15 NRS app users who felt comfortable, very comfortable, or neutral for sharing general receipts (AQ3-1) became uncomfortable or very uncomfortable for sharing receipts that contain sensitive information (AQ3-3). All of them expressed concerns on privacy or other potential risks, e.g., *"My level of comfortability changes when I think my sensitive information is at risk. Things that I might consider to be sensitive information might be my name, credit card information, phone number, etc. I'd feel much more comfortable sharing my receipts if I knew my personal information was safe"* (RS app user #39). Recall that we did observe these types of sensitive information in receipt transcription tasks as shown in Table 1 (Section 3.1.2).

Comfort level across different types of information. To explore how app users' feelings vary across different types of information on receipts that are accessible by anonymous individuals, we asked AQ3-5 with the results presented in Figure 4. We can see that in general app users were more uncomfortable with the disclosure of customers' (i.e., app users') information than vendors' (i.e., stores') information. NRS app users were more uncomfortable than RS app users with the disclosure of both customers' and vendors' information. RS app users expressed the most discomfort with a customer's home address (89.3%) and the least discomfort with a store's name (3.6%). Similarly, NRS app users expressed the most discomfort with a customer's home address (96.2%) and the least discomfort with a store's name (26.9%). For all types of information except for a credit card's last 4 digits, we observed statistically significant differences in comfort levels between RS and NRS app users by using the Wilcoxon rank sum tests. Surprisingly, most RS and NRS app users were uncomfortable or very uncomfortable with disclosing credit cards' last 4 digits, but that is one of the most common types of information on receipts as shown in Table 1. However, their concerns are not unfounded as credit cards' last 4 digits are widely used by fraudsters to launch smishing attacks, for example, Bankwest warned its customers in 2022 about the identified scams that use

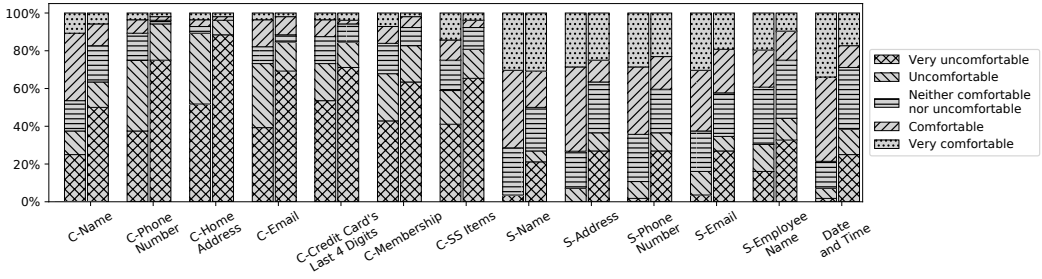


Fig. 4. Percentages of App Users Who Felt Comfortable Across Different Types of Information Present on Receipts and Visible to Anonymous Individuals (AQ3-5). C-: Customer, S-: Store, C-SS Items: Customer's Sensitive Shopping Items. For each type of information, the left bar is for RS app users, and the right bar is for NRS app users.

such information to develop trust with people in order to trick them to become victims [6]. In addition, many NRS app users were even concerned about the date and time information on receipts. This is also understandable as temporal context is usually essential in user privacy. Overall, it is clear that most RS and NRS app users do have strong concerns about having their own information on receipts accessible by anonymous individuals.

Opinions on protecting the information on receipts. Figure 5 shows the distributions of RS and NRS app users' agreements on the statements "*Protecting the privacy of customers on receipts is important.* (AQ4-1)" and "*Protecting the privacy of vendors on receipts is important.* (AQ4-2)". We found that 96.4% of RS app users and 98.1% of NRS app users somewhat agreed or strongly agreed that protecting receipt owners' privacy is important (AQ4-1). As for AQ4-2, 62.5% of RS app users and 67.3% of NRS app users somewhat agreed or strongly agreed on it. There is no statistically significant difference between RS and NRS app users regarding their agreements on protecting either vendors' or customers' privacy according to the Wilcoxon rank sum tests; the overwhelming agreement from both RS and NRS app users on AQ4-1 especially highlights the urgency of protecting receipt owners' privacy. In addition, app users also reported whether they expect an app itself or other parties to obscure the sensitive information on receipts. We observe that 60.7% of RS app users and 50.0% of NRS app users expected an app itself to obscure the sensitive information before transmitting receipts to other parties (AQ4-3); 53.6% of RS app users and 36.5% of NRS app users expected other parties to obscure sensitive information before distributing receipts to anonymous individuals (AQ4-4). Moreover, the majority of RS (75.0%) and NRS (84.6%) app users stated that they would obscure sensitive information before uploading their receipts (AQ4-5). Unfortunately, no protection is in place yet and it is extremely rare to observe receipts' information being obscured on MTurk (Section 3.1.2).

4.1.4 Summary of Findings in the App User Study. Three findings from Section 4.1.2 respond to RQ1: (1) the majority (58.9%) of RS app users believed that receipt information is extracted within an app itself locally whereas the majority (61.5%) of NRS app users doubted that (RQ1-1); (2) there is a higher percentage of RS than NRS app users who believed that their receipts will not be accessible by other parties and anonymous individuals (RQ1-2); (3) the differences between the answer distributions of RS and NRS app users on questions AQ2-1, AQ2-3, and AQ2-4 regarding their understanding of data extraction and sharing practices are statistically significant (RQ1-3). Overall, a considerable percentage of RS app users misunderstood the data extraction and sharing practices of RS apps, which might lead them to be less thoughtful of their privacy.

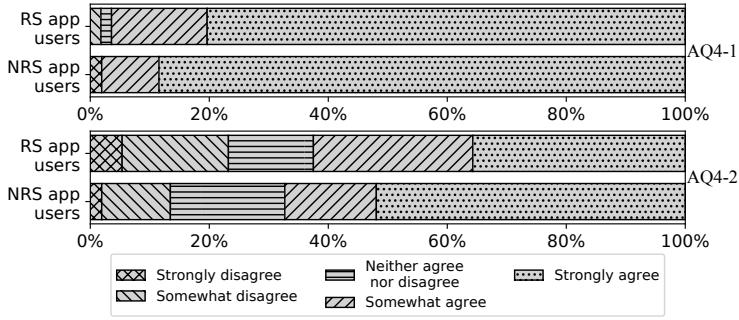


Fig. 5. App Users' Agreement Level on the Importance of Privacy Protection. (AQ4-1: Protecting the privacy of customers on receipts is important. AQ4-2: Protecting the privacy of vendors on receipts is important.)

Three findings from Section 4.1.3 respond to RQ2: (1) most RS (80.4%) and NRS (92.3%) app users have severe concerns about having their receipts with sensitive information transmitted to other parties and be accessible by anonymous individuals, and this is largely due to the worries on negative privacy or security consequences (RQ2-1); (2) 96.4% of RS app users and 98.1% of NRS app users agreed or strongly agreed with the importance of protecting the privacy of customers on receipts (RQ2-2); (3) NRS app users are more concerned than RS app users about the disclosure of their general receipts to other parties or anonymous individuals (RQ2-3). Overall, for receipts with sensitive information, both RS and NRS app users expressed severe concerns and strong desires for privacy protection.

4.2 Results of the Crowd Worker Study

We first present the demographics and MTurk work experiences of crowd workers. We then detail the results to answer RQ3 and RQ4.

4.2.1 Demographics and Work Experiences on MTurk. A total of 166 crowd workers took the survey in our crowd worker study. After filtering out 64 participants who answered the attention check question incorrectly or provided completely irrelevant answers to open-ended questions, we obtained valid responses from 102 crowd workers. Table 4 in Appendix B.2 summarizes the demographics of crowd workers and their general experiences on MTurk. In brief, 73.5% of crowd workers were between 18 and 39 years old. As for the gender, 62.7% of crowd workers identified themselves as male while 37.3% were female. Regarding their work experiences on MTurk, 81.4% of crowd workers claimed that MTurk provides their supplementary income while 18.6% considered it as their primary income source. Meanwhile, the majority (85.3%) of crowd workers reported working on MTurk for more than one year; 48.0% of crowd workers reported spending more than 20 hours per week on MTurk, and 42.2% reported spending between 10 and 20 hours per week.

4.2.2 RQ3: Crowd Workers' Opinions about Sensitivity of Receipts' Information and Experiences with Receipt Transcription Tasks.

Perceived sensitivity and relevant experience. Crowd workers were asked to select the types of information they considered as sensitive (TQ2-1) and then indicate whether they have ever seen the information in receipt transcription tasks (TQ2-2). As shown in Figure 6, a customer's phone number was considered sensitive by the most crowd workers (94.1%); it is followed by a customer's physical address (92.2%), email address (78.4%), name (71.6%), membership ID (47.1%), shopping items (45.1%), and credit card's last 4 digits (26.5%). Among a store's information, an employee's name

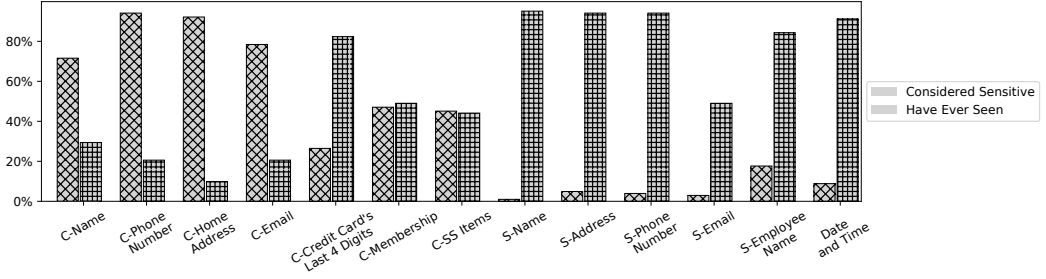


Fig. 6. Percentages of Crowd Workers Who Considered Some Types of Information as Sensitive (TQ2-1) and Who Have Ever Seen the Information in Receipt Transcription Tasks (TQ2-2). C-: Customer, S-: Store, C-SS Items: Customer's Sensitive Shopping Items.

was considered sensitive by the most crowd workers (17.6%). Overall, crowd workers considered customers' information to be more sensitive than vendors' information. Correlating to the results on AQ3-5 in Section 4.1.3, we can see that in general, the types of information that app users felt uncomfortable with are also what crowd workers considered as sensitive; one exception is a customer's credit card's last 4 digits - 73.2% of RS app users and 84.6% of NRS app users felt uncomfortable with it, while only 26.5% of crowd workers considered it sensitive.

As for TQ2-2, crowd workers have commonly seen most types of information of a store in receipt transcription tasks. For example, 95.1% and 84.3% of them have ever seen a store's name and a store employee's name, respectively. Meanwhile, it is clear that a noticeable percentage of crowd workers have seen customers' sensitive information (name, phone number, home address, email address, credit card's last 4 digits, membership ID, and shopping items by 29.4%, 20.6%, 9.8%, 20.6%, 82.4%, 49.0%, and 44.1% of crowd workers, respectively) in receipt transcription tasks. This result indicates that the disclosure of receipt owners' sensitive information is indeed prevalent on MTurk.

Experiences on transcription tasks. We further explored crowd workers' experiences on receipt transcription tasks including how often they view receipt transcription tasks with sensitive information on MTurk (TQ2-3) and on other crowdsourcing platforms (TQ2-4). Table 2 summarizes the results of those questions. For TQ2-3, 44.2% of crowd workers reported working on receipt transcription tasks that contain sensitive information at least monthly, indicating that the disclosure of sensitive information on receipts happens frequently on MTurk. For TQ2-4, 12.8% of crowd workers selected monthly or weekly, indicating that the disclosure of sensitive information on receipts also happens on other crowdsourcing platforms. It is worth noting that this low percentage on other crowdsourcing platforms is likely because we recruited crowd workers on MTurk and most of them mainly worked on this platform.

Crowd workers also reported the number of receipt transcription tasks they perform on average per week on MTurk (TQ3-1) and other types of transcription tasks that contain sensitive information of other people (TQ3-3). The results are also presented in Table 2. We can see that 47.1% of crowd workers worked on less than 10 receipt transcription tasks per week, and 30.4% of crowd workers worked on 10 or more receipt transcription tasks per week. As for other types of transcription tasks that contain sensitive information, 50.0%, 44.1%, 28.4%, and 18.6% of crowd workers mentioned invoice, business card, financial document, and court document transcriptions, respectively. This result is very concerning as these types of documents often contain their owners' detailed personal information such as name, home address, and sensitive financial information or activities. It confirms that the sensitive information of other people is disclosed not only in receipt transcription tasks

but also in other types of transcription tasks, demonstrating ***the broad scope of the privacy risks we investigate in this paper***. Note that we provided those check-box options in TQ3-3 because we also observed those types of transcription tasks on MTurk when we started the design of this crowd worker survey study.

Table 2. Crowd Workers' Experiences on Transcription Tasks. (RT: Receipt Transcription, HIT: Human Intelligence Task)

Crowd Workers (102)		Crowd Workers (102)	
Frequency on RT tasks with sensitive content (MTurk)		# receipt transcription HITs/week	
Daily	2(2.0%)	< 10 HITs/week	48(47.1%)
Weekly	15(14.7%)	10-49 HITs/week	21(20.6%)
Monthly	28(27.5%)	50-99 HITs/week	4(3.9%)
Yearly	25(24.5%)	100-199 HITs/week	4(3.9%)
Never	24(23.5%)	> 199 HITs/week	2(2.0%)
Other	8(7.8%)	None	18(17.6%)
Frequency on RT tasks with sensitive content (others)		Other transcription tasks	
Daily	1(1.0%)	Invoice	51(50.0%)
Weekly	2(2.0%)	Court Document	19(18.6%)
Monthly	11(10.8%)	Financial Document	29(28.4%)
Yearly	9(8.8%)	Business Card	45(44.1%)
Never	75(73.5%)	Resume	15(14.7%)
Other	4(3.9%)	None	14(13.7%)
		Other	7(6.9%)

4.2.3 RQ4: Crowd Workers' Attitudes Towards Privacy Problems in Receipt Transcription Tasks.

Opinions on protecting the information on receipts. Figure 7 shows the distributions of crowd workers' agreements on the statements "Protecting the privacy of customers on receipts is important. (TQ4-1)" and "Protecting the privacy of vendors on receipts is important. (TQ4-2)". We found that 99.0% of crowd workers somewhat agreed or strongly agreed with TQ4-1, indicating a strong need for protecting receipt owners' privacy. Only 37.3% of crowd workers somewhat agreed or strongly agreed with TQ4-2. The answer distribution difference between TQ4-1 and TQ4-2 is statistically significant based on the Wilcoxon signed rank test ($p < 0.05$).

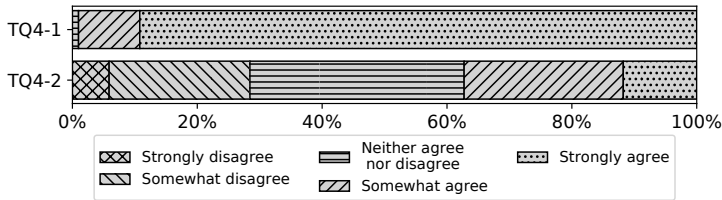


Fig. 7. Crowd Workers' Agreement Level on the Importance of Privacy Protection. (TQ4-1: Protecting the privacy of customers on receipts is important. TQ4-2: Protecting the privacy of vendors on receipts is important.)

Recall that we have two almost identical questions in the app user study (Section 4.1.3) showing that both RS and NRS app users had a high level of agreement with the need for protecting receipt owners' privacy. Although crowd workers had a slightly higher level of agreement on TQ4-1 than RS and NRS app users on AQ4-1, the difference among these three groups is not statistically

significant based on the Kruskal-Wallis test ($p > 0.05$), indicating that both crowd workers and app users agreed that protecting customers' privacy is important. As for the protection of vendors' privacy, crowd workers had a lower level of agreement on TQ4-2 than RS and NRS app users on AQ4-2. This difference is statistically significant based on the Kruskal-Wallis test ($p < 0.05$), and it can be explained by different perceptions of sensitivity to vendors' information: a considerable percentage of RS and NRS app users were uncomfortable with disclosing vendors' information while only a small percentage of crowd workers considered vendors' information sensitive.

Comfort level with receipt transcription tasks. Crowd workers reported how they feel about working on receipt transcription tasks that contain a customer's sensitive information (TQ4-4) and a vendor's sensitive information (TQ4-6); they also reported how they would feel about having their own receipts that contain sensitive information transcribed by other crowd workers (TQ4-8). Figure 8 shows the distributions of crowd workers' answers to these three questions. Only 43.1% of crowd workers were comfortable or very comfortable with working on receipt transcription tasks that contain a customer's sensitive information. Majority (78.4%) of crowd workers were comfortable with tasks that contain a vendor's sensitive information. However, only a very small percentage (11.8%) of crowd workers were comfortable or very comfortable with having their own receipts that contain sensitive information transcribed by other crowd workers. This big difference between crowd workers' comfort level with their own sensitive information (TQ4-8) and that with customers' sensitive information (TQ4-4) is statistically significant based on the Wilcoxon signed rank test. It implies that most crowd workers were clearly aware of the existence of customers' sensitive information on receipts; it also implies that people can be more cautious or conscientious about their own sensitive information than that of others. Overall, these results and the results from AQ3-3 (Section 4.1.3) show that both crowd workers and app users were concerned about having their own receipts with sensitive information accessible by anonymous individuals.

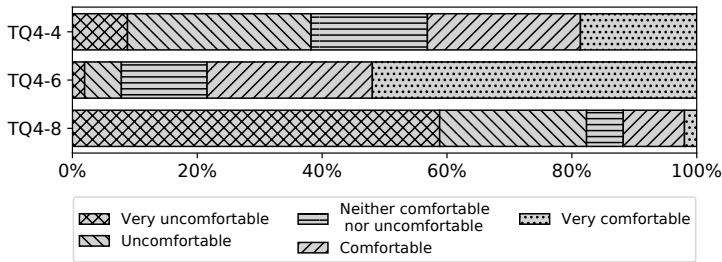


Fig. 8. Crowd Workers' Comfort Level for Transcribing Receipts with Sensitive Information of Customers (TQ4-4) and Vendors (TQ4-6), and for Having Their Own Receipts with Sensitive Information Transcribed by Other Workers (TQ4-8).

Reasons for comfort or discomfort. TQ4-5, TQ4-7, and TQ4-9 are open-ended questions that asked crowd workers to explain their answers to TQ4-4, TQ4-6, and TQ4-8, respectively.

Among 44 crowd workers who were comfortable or very comfortable with working on receipt transcription tasks that contain a customer's sensitive information (TQ4-4), 18 commented that they were trustworthy and would not misuse information of others, e.g., "I am comfortable because I am a trustworthy person. I would not share the information or use it in any way" (crowd worker #91); 12 mentioned that they merely focused on the tasks without paying attention to other information, e.g., "I feel comfortable because I am used to working on tasks that contain this information. I don't know if this is invasive for the customer, but I'm just doing what the task assigned to me is" (crowd

worker #28); six assumed that customers should have consented to post their receipts, e.g., *"If it was uploaded, then that customer must be satisfied and comfortable with uploading such information. I do not mind working on such tasks because I can be trusted to not use their information"* (crowd worker #3); five thought they were not responsible for customers' privacy, e.g., *"I don't care about others' privacy. They are irrelevant to me"* (crowd worker #2); two considered the information on receipts not sensitive, e.g., *"I don't think any of the information would be sensitive enough to help me identify the individual so it's not a big deal"* (crowd worker #46); one provided an irrelevant response. We can see that most of these crowd workers either considered themselves trustworthy or merely concentrated on completing tasks. However, we should note that their comfortableness and reasons do not guarantee that customers will be free of worry about their privacy.

Among 39 crowd workers who were uncomfortable or very uncomfortable on TQ4-4, 19 respected the privacy of customers and had concerns about privacy violation or invasion, e.g., *"It feels like I am accessing someone's personal information without their knowledge. It just gives me the feeling that I am invading someone's privacy and I don't like that"* (crowd worker #53); five revealed concerns about the lack of transparency, e.g., *"I worry about the customer's data safety/ignorance on how it's being used"* (crowd worker #56); five worried about other potential risks to customers, e.g., *"If I can see it, then some black hat could do something nefarious with it. The black hat could hack into that person's bank account"* (crowd worker #61); four were afraid of being blamed for incidents involving sensitive information, e.g., *"I'm always concerned that I might be blamed for some sort of incident if I had access to their information. I don't want to get in trouble or feel like I caused something"* (crowd worker #60); three wished to have the explicit consent from customers, e.g., *"Unless it's specifically mentioned that the person gave their consent for their information to be provided I really feel uncomfortable seeing sensitive information"* (crowd worker #9); three had other reasons. Although these crowd workers provided diverse reasons, most of them were concerned about the negative privacy or security consequences to customers. This aligns with why app users were concerned about having their receipts accessible to anonymous individuals as analyzed in Section 4.1.3.

As for the tasks that contain a vendor's sensitive information (TQ4-6), 80 crowd workers were comfortable or very comfortable. Among them, 50 considered the information of a vendor public or trivial, e.g., *"It is public information. It will be safe to use"* (crowd worker #7); nine had no concerns because they believed that vendors determined the information on receipts, e.g., *"I mean, the vendor made the program and receipt, so they can choose to have what's on there and what's not there. That's up to them"* (crowd worker #41); six mentioned that they could not perceive harms, e.g., *"I would feel comfortable because I don't see the harm in knowing info"* (crowd worker #30); four were comfortable if receipts do not contain sensitive information of employees, e.g., *"As long as it does not contain information too sensitive about individuals who work there I do not really care"* (crowd worker #31); four just would not mind, four mentioned that they merely focused on the tasks, and three had other reasons. Overall, most crowd workers did not consider vendors' information sensitive or important, and this aligns with the app users' overall sentiment on vendors' information as analyzed in Section 4.1.3. The major reasons from eight crowd workers who selected uncomfortable or very uncomfortable for TQ4-6 are similar to those for TQ4-4: three valued the privacy of vendors, one worried about being blamed, one worried about the unclear destination of the information, and three had other reasons.

When asked how they feel about having their own receipts with sensitive information transcribed by other workers (TQ4-8), only 12 crowd workers were comfortable or very comfortable. Among them, three considered the information on receipts trivial, e.g., *"It just doesn't seem like it would be a serious concern. Nothing on my receipts can be stolen and used for anything negative"* (crowd worker #46); three trusted other crowd workers, e.g., *"Mturk worker's are not using any of this information for nefarious purposes"* (crowd worker #4); three felt comfortable as long as the information is not

sensitive, e.g., *"It truly depends on what the sensitive information is. I do not care about my name or the last 4 digits of my card being shown. I care if my phone number or address is revealed and would never upload a receipt with that information"* (crowd worker #102); two thought that they already agreed with the transcription, e.g., *"If I were to upload a receipt then I already agree to their terms of service that these receipts could be processed or seen by others"* (crowd worker #14); one had other reasons.

Among 84 crowd workers who selected uncomfortable or very uncomfortable for TQ4-8, 26 valued their privacy and had concerns on privacy disclosure; 16 were just unwilling to share; 15 worried about other potential risks to them; five highlighted their concerns on being unclear how the information would be processed and used; three had other reasons; 19 explicitly mentioned distrust as the reason for discomfort, e.g., *"I am not sure if the workers are honest therefore I do not really trust them"* (crowd worker #48). While the major reasons are related to privacy concerns, it is interesting that distrust was explicitly brought out by 19 crowd workers. It is worth recalling that 18 crowd workers commented in TQ4-5 that they were trustworthy and thus comfortable with tasks containing sensitive information of customers. It is natural for people to have different opinions about themselves vs. others, but here this difference on trust matters and implies potential privacy risks to those RS app users who were simply unaware of the access of their receipts by anonymous individuals in the first place (Section 4.1.2). Moreover, the distrust of other workers is likely due to the anonymous nature of crowd workers, e.g., *"I do not trust others to keep my sensitive information private. I would not want any of my information released due to the poor control MTurk has over both workers and requesters, and their lack of service to both except in providing a gig-worker space where money changes hands. Especially because some of the people doing transcription work could be using that information for identity theft purposes, or the requester could be using it for ID theft, and there are many foreign and domestic workers that are essentially anonymous through MTurk that could take info"* (crowd worker #63).

Opinions on requesters of receipt transcription tasks. At the end of the survey, three open-ended questions were asked to explore crowd workers' understanding of the requesters' task purposes (TQ5-1), identities (TQ5-2), and receipt sources (TQ5-3).

Regarding how requesters will use receipt transcription results (TQ5-1), 27 crowd workers mentioned market exploration, e.g., *"Probably they want to find the pattern of people's purchasing habits. This data can be used to determine which items can gain traction in that particular area"* (crowd worker #17); 19 indeed linked receipt transcription tasks to RS apps and mentioned information verification, e.g., *"They are most likely verifying information for a company's rewards program, something like Ibotta"* (crowd worker #26); 16 mentioned receipt digitization or management, e.g., *"They will use it to digitally store data for their account records. This is to save physical space"* (crowd worker #45); 10 mentioned AI model training or development, e.g., *"I imagine they use this to train AI to do the job as well"* (crowd worker #1); six mentioned general research purposes; four considered malicious purposes, e.g., *"i think there is a potential for identity theft or other improper uses of this sensitive information"* (crowd worker #34); 14 were unsure about the purposes of those tasks, e.g., *"I have no idea and it's none of my concern once I've been paid for my time"* (crowd worker #6); six had other answers. The mentioned purposes are largely benign and are for supporting services or functionalities, which are consistent with our overall impression of receipt transcription tasks (Section 3.1) and RS apps (Section 2.1); meanwhile, it is encouraging to see that a considerable percentage (18.6%) of crowd workers were clearly aware of the connection between the app user community and the crowd worker community, which is in line with what we analyzed in Section 3.1.1.

Regarding who are the requesters of receipt transcription tasks (TQ5-2), crowd workers' responses are well aligned with the task purposes (TQ5-1). Specifically, 17 crowd workers listed the names of

some popular requesters on MTurk such as “Ibotta, Inc”; 14 thought the requesters would generally be RS app providers; 12 answered data analytic companies; 10 answered market exploration companies; nine answered vendors or small business owners; six answered researchers; four answered AI model developers; 17 were unsure about the task requesters; 13 had other answers.

Regarding how (i.e., from where or whom) task requesters obtained those receipts (TQ5-3), 30 crowd workers mentioned sources related to RS app providers, e.g., *“I believe that some of the requesters who post receipt transcription tasks obtain their receipts through apps that consumers use to scan their receipts to earn rebates, coupons, and other shopping incentives, such as apps like Ibotta”* (crowd worker #36); 17 mentioned customers such as from what they discarded, e.g., *“I would assume most of it is thrown on the ground or out as trash”* (crowd worker #16); 14 mentioned vendors, e.g., *“Perhaps sent to them by vendors who need this data stored on a computer. They’re contracted”* (crowd worker #1); 11 mentioned reward programs, e.g., *“They probably offered a stipend to individuals willing to provide the receipts”* (crowd worker #70); nine mentioned other crowd workers, e.g., *“They probably got it from MTURK from other MTURK workers”* (crowd worker #2); six mentioned online services, e.g., *“Through online media”* (crowd worker #69); 10 were unsure about the sources; five had other answers. The fact that a considerable percentage (29.4%) of crowd workers considered RS apps as the major source of receipt images on MTurk further confirms the connection between the app user community and the crowd worker community as we analyzed in Section 3.1.1.

4.2.4 Summary of Findings in the Crowd Worker Study. Three findings from Section 4.2.2 respond to RQ3: (1) in general, the types of information that app users felt uncomfortable with are also what crowd workers considered as sensitive (and similarly with customers’ information being more sensitive than vendors’ information) (RQ3-1); (2) 44.2% of crowd workers reported working on receipt transcription tasks that contain sensitive information at least monthly (RQ3-2); (3) a considerable percentage of crowd workers have seen other types of transcription (e.g., invoice, business card, financial document, and court document transcription) tasks that contain sensitive information of other people (RQ3-3). Overall, these findings demonstrate the prevalence of third parties’ privacy disclosure on MTurk and the broad scope of the privacy risks we investigate in this paper.

Four findings from Section 4.2.3 respond to RQ4: (1) 99.0% of crowd workers agreed or strongly agreed with the importance of protecting the privacy of customers on receipts (RQ4-1); (2) only 43.1% of crowd workers were comfortable or very comfortable with working on receipt transcription tasks that contain a customer’s sensitive information, and this is largely due to the worries on negative privacy or security consequences (similar to the reasons provided by app users as analyzed in Section 4.1.3) (RQ4-2); (3) only a very small percentage (11.8%) of crowd workers were comfortable or very comfortable with having their own receipts that contain sensitive information transcribed by other crowd workers, and this is largely due to the worries on negative privacy or other consequences as well as the distrust of other crowd workers (RQ4-3); (4) receipt transcription tasks were largely considered as being for benign purposes, 18.6% of crowd workers were clearly aware of the connection between the app user and the crowd worker communities, and 29.4% of crowd workers considered RS apps as the major source of the receipt images on MTurk (RQ4-4). Overall, while continuously working on those largely benign receipt transcription tasks, most crowd workers also expressed severe concerns and strong desires (similar to that from RS and NRS app users as summarized in Section 4.1.4) for protecting the privacy of customers on receipts.

5 DISCUSSIONS

We first discuss the implications of our key findings and provide our recommendations to stakeholders including RS app providers, app users, crowdsourcing platforms, and task requesters. We then discuss the limitations of this work and the potential future work.

5.1 Implications and Recommendations

Mismatches between app users' understanding and the reality. Our key findings summarized in Section 4.1.4 show that a considerable percentage of RS app users misunderstood the data extraction and sharing practices of RS apps. In the process of deriving those key findings, we analyzed the network traffic behaviors and privacy policies of 14 major RS apps (11 are what we identified for AQ1-3 and three are what RS app users further specified for AQ1-3) in terms of data transferring, sharing, and processing practices as shown in Table 5 in Appendix C.1. Using the VPN-based PCAPdroid network monitor [51], we observed that most (12 out of 14) apps have large payloads transferred to remote servers whenever we use their in-app camera function to take a photo of a receipt of ours, which indicates that they do send receipt images to remote servers for processing. Recall that in Section 4.1.2, the majority of RS app users believed that receipt information is extracted within an app itself locally, which might lead them to be less thoughtful of their privacy with respect to using RS apps. Such mismatches between RS app users' understanding of data extraction or collection practices and the reality are consistent with what some other researchers (e.g., Shklovski et al. [61]) found about the mismatches between app users' understanding of data collection and the actual rampant data collection.

Manually analyzing their privacy policies, we found that most (13 out of 14) apps indicated that they may share the collected data with third parties. However, only four apps' privacy policies explicitly mentioned who may process users' data such as receipts. Among them, two apps (Amazon Shopper Panel and Smart Receipts) indicated the human involvement in data processing. These results are concerning as most privacy policies do not sufficiently inform app users about the data processing practices and the potential risks of having their receipts accessible to anonymous individuals. Such insufficiency or lack of transparency in privacy policies could be a non-negligible factor contributed to many RS app users' misunderstanding that their receipts will not be accessible by other parties and anonymous individuals (Section 4.1.2), which might also lead them to be less thoughtful of their privacy with respect to using RS apps.

We recommend **RS app providers** to provide more transparency of their data collection, sharing, and processing practices to app users, including complementing their privacy policies with clear information regarding if other parties and anonymous individuals such as crowd workers may access the uploaded receipts. On the other hand, recall in Section 4.1.1 that most (66.1%) of RS app users claimed that they did not read the privacy policies of RS apps (AQ1-6). Therefore, we also recommend **app users** to be more attentive to privacy policies before installing and using RS apps. Especially considering that RS app users explicitly initiate receipt scanning actions, they are already aware of the basic fact of the apps' access to their receipts and they should go at least one step further to think or read about the potential follow-up privacy risks.

Privacy regulation compliance analysis. As shown in Section 3.1.1, the connection between the app user community and the crowd worker community is based on the sharing of receipt images. We introduced in Section 1.1 that widespread collection, aggregation, and dissemination of either e-receipts or physical receipts are apparently violating the regulations such as GDPR [24] and CCPA [8]. Our key findings summarized in Section 4.2.4 demonstrate the prevalence of third parties' privacy disclosure on MTurk and the broad scope of the privacy risks we investigate in this paper. We cannot imagine that RS apps and their practices to (either intentionally or unintentionally

via other parties) share potentially sensitive personal information quasi-publicly on crowdsourcing platforms can be compliant with GDPR or CCPA in any way. Even if app providers might be unaware of the violation of privacy regulations caused by other parties' posting of receipts on crowdsourcing platforms, it does not absolve app providers of their responsibility especially in case they did not explicitly require other parties to be GDPR or CCPA compliant in crowd-based data processing. As we observed that receipts (and correspondingly RS app users) came from many countries (Section 3.1.1), similar privacy regulation compliance problems likely exist in non-EU and non-USA countries based on their own specific regulations. We would recommend ***crowdsourcing platforms, RS app providers, and task requesters*** to more seriously consider and address the potential privacy regulation violations by working with their legal teams.

Privacy concerns of crowd-powered data processing. Although the privacy risks of general mobile app users have been intensively studied as reviewed in Section 2.2, our work is the first to investigate the privacy risks of millions of RS app users in the context of crowd-powered processing of their receipts. Previous studies such as [20, 44] have shown that sharing users' typical types of data such as contact and location data to the commonly known third parties such as advertisers and service providers is very concerning to app users. Our key findings summarized in Section 4.1.4 show that severe privacy concerns and strong desires for privacy protection also exist from both RS and NRS app users in the context of crowd-powered transcription of users' receipts. Meanwhile, our work is the first to formally investigate crowd workers' experiences and attitudes on realistic receipt transcription tasks on open crowdsourcing platforms. Our key findings summarized in Section 4.2.4 show that most crowd workers expressed severe privacy concerns and strong desires for privacy protection on receipt transcription tasks, although they continuously worked on those tasks. This phenomenon reveals a new type of "privacy paradox" that was not identified before (e.g., in [25, 36]) as it is about a paradoxical dichotomy between crowd workers' attitudes and behaviors towards other people's sensitive data. Therefore, we would recommend ***crowdsourcing platforms and task requesters*** to explore solutions to help crowd workers resolve this privacy paradox and become more comfortable on completing receipt transcription tasks. We will briefly discuss two possible solutions at the end of Section 5.2.

Responsible disclosure of our findings. We have disclosed our findings to Amazon researchers, and their MTurk team is conducting internal investigations. We have also disclosed our findings to the providers of all 14 RS apps (as listed in Table 5 in Appendix C.1) using their contact information on the Google Play Store; five providers acknowledged our disclosure effort with human responses (and one of them also asked for our full research paper), five other providers confirmed the receipt of our disclosure emails with auto-responses, but unfortunately the remaining four did not respond to us (after we emailed each of them twice). We would recommend ***RS app providers*** to be more responsive of researchers' privacy or security related responsible disclosure communication to them, and be more active in the protection of their users.

5.2 Limitations and Future Work

The crowdsourcing platform perspective. According to the acceptable usage policy of MTurk [1], "posting HITs that contain personal information of third parties" is prohibited. However, receipt transcription tasks have been continuously posted on MTurk on a daily basis, and they represent one major type of tasks (accounting for around 15.1% of viewable HIT groups on MTurk as shown in Section 3.1.2). Receipt and other types of transcription tasks often contain other people's sensitive information, raising severe privacy concerns as shown in our two user studies. To us, those task requesters apparently violated the usage policy of MTurk.

Many questions arise from the crowdsourcing platform perspective. Some examples are: Why has MTurk not taken actions to regulate the posting of receipt and other types of transcription tasks

that contain sensitive information of third parties? Is MTurk not aware of the potential privacy risks in the first place? Or, is MTurk simply unable to come up with an effective solution to address the challenges on allowing or facilitating useful transcription tasks while sufficiently preserving third party users' privacy? Although we could not answer all these questions in this work, we have already fully disclosed our findings to Amazon researchers for their internal investigations (Section 5.1). In the future, researchers may further explore the answers to these questions, and they may also go beyond MTurk by considering other crowdsourcing platforms.

The app provider perspective. Many questions from the app provider (or developer) perspective could not be answered by our work. For one example, it is unclear how RS app providers perceive the disclosing of app users' receipts on crowdsourcing platforms, and if they are willing to protect the sensitive information of receipt owners. As described above in Section 5.1, only five RS app providers acknowledged our responsible disclosure effort with human responses, indicating to a limited extent their care about their users. Meanwhile, our communication with them was purely for responsible disclosure instead of for formally soliciting in-depth responses from them. Therefore, conducting a formal user study on the providers of some of those hundreds of RS apps (Section 2.1) could be an interesting and beneficial future work, although we anticipate that recruiting participants would be a very challenging task.

For another example, it is unclear whether and how RS app providers are partnered with task requesters or data brokers. Meanwhile, although we know from our observation (Section 3.1.2) and crowd workers' responses (Section 4.2.2) that some RS app providers (e.g., Ibotta) continuously launch receipt transcription tasks on MTurk, it remains unclear to us whether partial or all receipts collected by those RS apps are manually transcribed. We conjecture that app providers may primarily take the AI-based automated receipt transcription (i.e., image and text recognition) approach, and may secondarily but often necessarily leverage the crowd-based manual transcription approach on complicated or periodically sampled receipts for quality assurance or improvement. AI-based automation is likely the primary approach due to two clues. One is that the number of receipt images posted on the major crowdsourcing platform MTurk is much smaller than the number of receipts that could be uploaded by millions of RS app users (Section 2.1). The other is that after receipt images are sent by some RS apps to their remote servers (Section 5.1), transcription results can often be returned within seconds. Crowdsourcing is likely the secondary but often necessary approach because AI models could be inaccurate especially on complicated or new styles of receipts, while manual transcription can help address individual problems and help improve AI models. Verifying this conjecture and ascertaining how RS app providers exactly leverage crowdsourcing could also be an interesting future work beneficial to the protection of app users' privacy.

The task requester perspective. Our work does not cover the opinions and privacy concerns from the task requester perspective as it is difficult to recruit or engage task requesters in the first place. We obtained some useful information from crowd workers regarding their understanding of the requesters' task purposes, identities, and receipt sources (Section 4.2.3). Meanwhile, some major requesters continuously post receipt transcription tasks and they are related to some popular RS apps (Section 3.1.1). However, it could be helpful for future research to obtain more information directly from task requesters regarding their opinions and suggestions.

The participant recruitment perspective. We acknowledge that biases exist in the participant recruitment of our work. For example, we did not screen participants based on the age, and 48.2% of our recruited RS app users were between 18 and 24 years old (Section 4.1.1). While this age information likely indicates that RS apps are more widely adopted among younger users, it would be better if we could intentionally recruit more participants from other age groups to have a more representative participant population. Besides, in our crowd worker study, the participant recruitment was only from MTurk; more broadly recruiting workers from multiple crowdsourcing

platforms to investigate and compare their experiences and attitudes on receipt as well as other types of transcription tasks will be valuable in the future.

The possible solution perspective. Similar to crowdsourcing platforms, task requesters face the challenges on being able to post transcription tasks (which are largely benign as analyzed in Section 4.2.3) while sufficiently preserving third party users' privacy. Note that we consider that crowdsourcing platforms also have the motivations to address the challenges for reasons such as better complying with privacy regulations or better marketing their privacy-preserving service capabilities. However, the reality is that neither crowdsourcing platforms nor task requesters appear to have found good solutions to address the challenges. In this work, we could not come up any good solution either, and can at most briefly outline two possible solutions as follows.

One naive solution is for either task requesters or crowdsourcing platforms to obfuscate (at their server-side) the sensitive content on receipts or other types of documents before making the tasks accessible to crowd workers. However, it will not always be easy to accurately locate the sensitive content, and obfuscation may affect the utility of the transcription results. Another possible but not easily achievable server-side solution is to segment each receipt image or document into small pieces, and then assign each piece as a microtask to a different worker [34]. With some clever design, this solution can make it very difficult for an individual worker to aggregate or deduce the sensitive information of a specific user. However, care must be taken in the detailed design because using microtasks may increase the overall cost of a task, improper segmentation may reduce the overall transcription quality, and multiple workers may still collude to obtain users' sensitive information. We hope future research can further explore these and other possible solutions to sufficiently protect third party users' privacy on crowdsourcing platforms.

6 CONCLUSION

In this paper, we investigated the privacy risks of third party app users in crowdsourcing and considered the case of receipt transcription for analysis. We designed and conducted (1) the app user study to explore how app users perceive privacy while using RS apps, and (2) the crowd worker study to investigate crowd workers' experiences on receipt transcription tasks and their attitudes towards such tasks. Overall, we found that most app users and crowd workers expressed strong concerns about the potential privacy risks to receipt owners, and they also had a very high level of agreement with the need for protecting receipt owners' privacy. We further discussed the implications of our key findings and provided our recommendations to stakeholders. We also discussed the limitations of this work and the potential future work for protecting third parties' privacy on crowdsourcing systems.

ACKNOWLEDGMENTS

We thank anonymous reviewers for their valuable suggestions. This research was partially supported by the NSF grant OIA-1936968 and the NSF grant CNS-2246143.

REFERENCES

- [1] Acceptable Use Policy of MTurks 2018. Acceptable Use Policy of MTurk. <https://www.mturk.com/acceptable-use-policy>.
- [2] Yuvraj Agarwal and Malcolm Hall. 2013. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceedings of the International Conference on Mobile systems, Applications, and Services (MobiSys)*.
- [3] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. 2020. "I am uncomfortable sharing what I can't see": Privacy Concerns of the Visually Impaired with Camera Based Assistive Applications. In *Proceedings of the USENIX Security Symposium (USENIX Security)*.
- [4] Maximilian Altmeyer, Pascal Lessel, and Antonio Krüger. 2016. Expense control: A gamified, semi-automated, crowd-based approach for receipt capturing. In *Proceedings of the International Conference on Intelligent User Interfaces*.

(UI).

- [5] Brandon Amos, Bartosz Ludwiczuk, Mahadev Satyanarayanan, et al. 2016. Openface: A general-purpose face recognition library with mobile applications. *CMU School of Computer Science Technical Report* (2016).
- [6] Bankwest-Scammers 2022. Bankwest text warning: 'Scammers have last 4 digits of your card number'. <https://au.finance.yahoo.com/news/banks-text-warning-scammers-have-last-4-digits-of-your-card-number-234255113.html>.
- [7] Virginia Braun and Victoria Clarke. 2006. Using Thematic Analysis in Psychology. *Qualitative Research in Psychology* 3, 2 (2006), 77–101.
- [8] CCPA 2018. G. DATA BROKERS AND THE CCPA. <https://oag.ca.gov/privacy/ccpa>.
- [9] Yan Chen, Andrés Monroy-Hernández, Ian Wehrman, Steve Oney, Walter S Lasecki, and Rajan Vaish. 2020. Sifter: A Hybrid Workflow for Theme-based Video Curation at Scale. In *ACM International Conference on Interactive Media Experiences*.
- [10] Justin Cranshaw, Emad Elwany, Todd Newman, Rafal Kocielnik, Bowen Yu, Sandeep Soni, Jaime Teevan, and Andrés Monroy-Hernández. 2017. Calendar.Help: Designing a Workflow-Based Scheduling Agent with Humans in the Loop. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.
- [11] Lee J Cronbach. 1951. Coefficient alpha and the internal structure of tests. *psychometrika* (1951).
- [12] Anupam Das, Nikita Borisov, and Matthew Caesar. 2014. Do You Hear What I Hear?: Fingerprinting Smart Devices Through Embedded Acoustic Components. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*.
- [13] Anupam Das, Nikita Borisov, and Matthew Caesar. 2016. Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.
- [14] Sanorita Dey, Nirupam Roy, Wenyuan Xu, Romit Roy Choudhury, and Srihari Nelakuditi. 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.
- [15] E-Receipts 2018. E-receipts from leading retailers 'may break data protection rules'. <https://www.theguardian.com/business/2018/dec/11/e-receipts-from-major-retailers-may-break-data-protection-rules-which>.
- [16] Peter Eckersley. 2010. How Unique is Your Web Browser?. In *Proceedings of the Privacy Enhancing Technologies Symposium (PETS)*.
- [17] Daniel Esser, Klemens Muthmann, and Daniel Schuster. 2013. Information extraction efficiency of business documents captured with smartphones and tablets. In *Proceedings of the ACM Symposium on Document Engineering (DocEng)*.
- [18] ExifViewer 2022. Exif Viewer Firefox Browser Extension. <https://addons.mozilla.org/en-US/firefox/addon/exif-viewer/>.
- [19] Expensify-MTurk-Case 2017. It's Not Always AI That Sifts Through Your Sensitive Info. <https://www.wired.com/story/not-always-ai-that-sifts-through-sensitive-info-crowdsourced-labor/>.
- [20] Adrienne Porter Felt, Serge Egelman, and David Wagner. 2012. I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proceedings of the ACM workshop on Security and Privacy in Smartphones and Mobile Devices*.
- [21] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
- [22] Casey Fiesler and Blake Hallinan. 2018. "We Are the Product" Public Reactions to Online Data Sharing and Privacy Controversies in the Media. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.
- [23] Sandra Gabriele and Sonia Chiasson. 2020. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.
- [24] GDPR 2018. Personal Data - General Data Protection Regulation (GDPR). <https://gdpr-info.eu/issues/personal-data/>.
- [25] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* (2018).
- [26] Google Assistant Service 2019. Google ordered to halt human review of voice AI recordings over privacy risks. <https://techcrunch.com/2019/08/02/google-ordered-to-halt-human-review-of-voice-ai-recordings-over-privacy-risks/>.
- [27] Danna Gurari, Qing Li, Chi Lin, Yinan Zhao, Anhong Guo, Abigale Stangl, and Jeffrey P Bigham. 2019. Vizwiz-priv: A dataset for recognizing the presence and purpose of private visual information in images taken by blind people. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*.
- [28] Alexander Heinrich, Matthias Hollick, Thomas Schneider, Milan Stute, and Christian Weinert. 2021. PrivateDrop: Practical Privacy-Preserving Authentication for Apple AirDrop. In *Proceedings of the USENIX Security Symposium*.
- [29] Zheng Huang, Kai Chen, Jianhua He, Xiang Bai, Dimosthenis Karatzas, Shijian Lu, and CV Jawahar. 2019. Icdar2019 competition on scanned receipt ocr and information extraction. In *Proceedings of the International Conference on Document Analysis and Recognition (ICDAR)*.
- [30] Thomas Hupperich, Davide Maiorca, Marc Kührer, Thorsten Holz, and Giorgio Giacinto. 2015. On the Robustness of Mobile Device Fingerprinting: Can Mobile Users Escape Modern Web-Tracking Mechanisms?. In *Proceedings of the*

Computer Security Applications Conference (ACSAC).

- [31] Farnaz Jahanbakhsh, Elnaz Nouri, Robert Sim, Ryen W. White, and Adam Fourney. 2022. Understanding Questions that Arise When Working with Business Documents. In *Proceedings of the ACM Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)*.
- [32] Nan Jiang, Yi Zhuang, and Dickson KW Chiu. 2020. Effective and efficient crowd-assisted similarity retrieval of medical images in resource-constraint Mobile telemedicine systems. *Multimedia Tools and Applications* (2020).
- [33] Thivya Kandappu, Vijay Sivaraman, Arik Friedman, and Roksana Boreli. 2014. Loki: a privacy-conscious platform for crowdsourced surveys. In *Proceedings of the International Conference on Communication Systems and Networks (COMSNETS)*.
- [34] Harmanpreet Kaur, Mitchell L. Gordon, Yiwei Yang, Jeffrey P. Bigham, Jaime Teevan, Ece Kamar, and Walter S. Lasecki. 2017. CrowdMask: Using Crowds to Preserve Privacy in Crowd-Powered Systems via Progressive Filtering. In *Proceedings of the AAAI Conference on Human Computation and Crowdsourcing (HCOMP)*.
- [35] Aniket Kittur, Jeffrey V Nickerson, Michael Bernstein, Elizabeth Gerber, Aaron Shaw, John Zimmerman, Matt Lease, and John Horton. 2013. The future of crowd work. In *Proceedings of the Conference on Computer Supported Cooperative Work (CSCW)*.
- [36] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* (2017).
- [37] Klaus Krippendorff. 2018. *Content Analysis: An Introduction to Its Methodology*. SAGE Publications; 4th Edition.
- [38] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. ‘No Telling Passcodes Out Because They’re Private’: Understanding Children’s Mental Models of Privacy and Security Online. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 64 (2017).
- [39] Walter S. Lasecki, Jaime Teevan, and Ece Kamar. 2014. Information Extraction and Manipulation Threats in Crowd-Powered Systems. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*.
- [40] Matthew Lease, Jessica Hullman, Jeffrey Bigham, Michael Bernstein, Juho Kim, Walter Lasecki, Saeideh Bakhshi, Tanushree Mitra, and Robert Miller. 2013. Mechanical turk is not anonymous. *Social Science Research Network* (2013).
- [41] Hwansoo Lee, Dongwon Lim, Hyerin Kim, Hangjung Zo, and Andrew P Ciganek. 2015. Compensation paradox: the influence of monetary rewards on user behaviour. *Behaviour & Information Technology* (2015).
- [42] Christophe Leung, Jingjing Ren, David Choffnes, and Christo Wilson. 2016. Should You Use the App for That?: Comparing the Privacy Implications of App- and Web-based Online Services. In *Proceedings of the Internet Measurement Conference (IMC)*.
- [43] Yifang Li, Nishant Vishwamitra, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. 2017. Effectiveness and users’ experience of obfuscation as a privacy-enhancing technology for sharing photos. *Proceedings of the ACM on Human-Computer Interaction (CSCW)* (2017).
- [44] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: understanding users’ mental models of mobile app privacy through crowdsourcing. In *Proceedings of the ACM Conference on Ubiquitous Computing (UbiComp)*.
- [45] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhammedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. 2016. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.
- [46] Raymond Madden. 2017. *Being Ethnographic: A Guide to the Theory and Practice of Ethnography*. SAGE Publications; 2nd Edition.
- [47] Gary Marchionini. 2006. Exploratory Search: From Finding to Understanding. *Commun. ACM* 49, 4 (2006), 41–46.
- [48] Tamir Mendel and Eran Toch. 2017. Susceptibility to social influence of privacy behaviors: Peer versus authoritative sources. In *Proceedings of the ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW)*.
- [49] MTurk-Alternatives 2022. 16 Best Amazon MTurk Alternatives To Make More Money Online. <https://thisonlineworld.com/mturk-alternatives/>.
- [50] Amy Pavel, Colorado Reed, Björn Hartmann, and Maneesh Agrawala. 2014. Video digests: a browsable, skimmable format for informational lecture videos. In *Proceedings of the ACM Symposium on User Interface Software and Technology*.
- [51] PCAPdroid 2022. PCAPdroid User Guid. <https://emanuele-f.github.io/PCAPdroid/>.
- [52] Weiping Pei, Arthur Mayer, Kaylynn Tu, and Chuan Yue. 2020. Attention please: Your attention check questions in survey studies can be automatically answered. In *Proceedings of The Web Conference*.
- [53] Weiping Pei, Zhiju Yang, Monchu Chen, and Chuan Yue. 2021. Quality Control in Crowdsourcing based on Fine-Grained Behavioral Features. *Proceedings of the ACM on Human-Computer Interaction (CSCW)* (2021).
- [54] Privacy-or-Planet 2021. Column: Privacy or planet - the tough choice of doing away with paper receipts. <https://www.latimes.com/business/story/2021-03-02/column-consumers-paper-receipts-environment>.

- [55] Jingjing Ren, Ashwin Rao, Martina Lindorfer, Arnaud Legout, and David Choffnes. 2016. Recon: Revealing and controlling pii leaks in mobile network traffic. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*.
- [56] Jonathan Robinson, Cheskie Rosenzweig, Aaron J Moss, and Leib Litman. 2019. Tapped out or barely tapped? Recommendations for how to harness the vast and largely unused potential of the Mechanical Turk participant pool. *PLoS one* (2019).
- [57] Sebastian Roth, Lea Gröber, Michael Backes, Katharina Krombholz, and Ben Stock. 2021. 12 Angry Developers - A Qualitative Study on Developers' Struggles with CSP. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. 3085–3103.
- [58] Beatriz Sainz-De-Abajo, José Manuel García-Alonso, José Javier Berrocal-Olmeda, Sergio Laso-Mangas, and Isabel De La Torre-Díez. 2020. FoodScan: Food Monitoring App by Scanning the Groceries Receipts. *IEEE Access* (2020).
- [59] Shruti Sannon and Dan Cosley. 2018. "It was a shady HIT" Navigating Work-Related Privacy Concerns on MTurk. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA)*.
- [60] Shruti Sannon and Dan Cosley. 2019. Privacy, power, and invisible labor on Amazon Mechanical Turk. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI)*.
- [61] Irina Shklovski, Scott D Mainwaring, Halla Hrunn Skúladóttir, and Höskuldur Borgthorsson. 2014. Leakiness and Creepiness in App Space: Perceptions of Privacy and Mobile App Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.
- [62] Anastasia Shuba, Athina Markopoulou, and Zubair Shafiq. 2018. NoMoAds: Effective and Efficient Cross-App Mobile Ad-Blocking. In *Proceedings of the Privacy Enhancing Technologies Symposium (PETS)*.
- [63] Saiganesh Swaminathan, Raymond Fok, Fanglin Chen, Ting-Hao (Kenneth) Huang, Irene Lin, Rohan Jadvani, Walter S. Lasecki, and Jeffrey P. Bigham. 2017. WearMail: On-the-Go Access to Information in Your Email with a Privacy-Preserving Human Computation Workflow. In *Proceedings of the ACM Symposium on User Interface Software and Technology (UIST)*. 807–815.
- [64] Aditya Vashistha, Pooja Sethi, and Richard Anderson. 2017. Respeak: A voice-based, crowd-powered speech transcription system. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*.
- [65] Huichuan Xia, Yang Wang, Yun Huang, and Anuj Shah. 2017. "Our Privacy Needs to Be Protected at All Costs": Crowd Workers' Privacy Experiences on Amazon Mechanical Turk. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 113 (2017).
- [66] Paul Yoder, Frank J. Symons, and Blair P. Lloyd. 2018. *Observational Measurement of Behavior*. Brookes Publishing; Second Edition.
- [67] Miuyin Yong Wong, Matthew Landen, Manos Antonakakis, Douglas M. Blough, Elissa M. Redmiles, and Mustaque Ahamad. 2021. An Inside Look into the Practice of Malware Analysis. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. 3053–3069.
- [68] Chen Jason Zhang, Ziyuan Zhao, Lei Chen, Hosagrahar Visvesvaraya Jagadish, and Chen Caleb Cao. 2014. Crowd-matcher: crowd-assisted schema matching. In *Proceedings of the ACM SIGMOD International Conference on Management of Data*.
- [69] Daniel Yue Zhang, Yifeng Huang, Yang Zhang, and Dong Wang. 2020. Crowd-assisted disaster scene assessment with human-ai interactive attention. In *Proceedings of the AAAI Conference on Artificial Intelligence*.
- [70] Guangyu Zhu, Timothy J Bethea, and Vikas Krishna. 2007. Extracting relevant named entities for automated expense reimbursement. In *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*.

A APPENDIX

A.1 App User Survey

We recruited two groups of app users in this survey: RS app users who have experience in using some receipt scanning app(s), and NRS app users who have not used any receipt scanning app yet. In this paper, we use the AQ prefix to number the survey questions asked to app users. We first asked participants to take a screening survey to determine their eligibility (e.g., they must be adults in the U.S.) for this survey and determine if they are RS vs. NRS app users. The follow-up survey questions for each group were the same except that two app usage related questions, AQ1-5 and AQ1-6 (denoted by a ★), were not shown to NRS app users. With their consent to participate in this survey study, app users were presented with the following 26 (24 for NRS app users) questions. We list them in five sets (i.e., AQ1- to AQ5-) and added notes in bold font before each set to improve

the readability of the paper. Demographics related questions are not listed here due to the space limitation, but the results are summarized at the end of this appendix.

AQ1-1 to AQ1-6: These questions are about whether a participant has used some receipt scanning app(s) before and how often and long is the usage.

AQ1-1. Have you ever shared your receipts to some websites or apps?

- Yes ◦ No ◦ Not sure

AQ1-2. (Note this question is displayed depending on a participant's answer to AQ1-1.)

You answered "Yes" on the previous question. Please explain why you use receipt scanning apps.

You answered "No" on the previous question. Please explain why you don't use receipt scanning apps.

You answered "Not sure" on the previous question. Please explain why you don't use receipt scanning apps.

Please write at least two sentences for your response.

AQ1-3. Which of the following apps have you used to upload your receipts? (Please select all that apply)

- ☐ Expensify
- ☐ Quickbooks
- ☐ Receipt Hog
- ☐ Shopkick
- ☐ Receipt Pal
- ☐ Smart Receipts
- ☐ Receipt Bank (Dext)
- ☐ Zoho Expense
- ☐ Ibotta
- ☐ Fetch
- ☐ CoinOut
- ☐ Other (please specify)
- ☐ None of the above

AQ1-4. How long have you been uploading receipts to apps that you checked in the above question?

- More than 1 year
- Around 1 year
- Less than 1 year
- Couple of months
- Few weeks
- Not applicable

★AQ1-5. On average, how often do you use receipt scanning apps?

- More than once a day
- Once a day
- More than once a week
- Once a week
- More than once a month
- Once a month
- More than once a year
- Once a year
- Never

★AQ1-6. Have you ever read the privacy policy of receipt scanning apps?

- Yes ○ No ○ Other (please specify)

AQ2-1 to AQ2-5: These questions are about app users' understanding of data extraction and sharing practices of receipt scanning apps.

Since NRS app users may not know receipt scanning apps, we provided one of the following two prompts randomly just to them:

Rewards App prompt: Suppose there is an application for smartphones that helps you earn cash back on everyday purchases like groceries, apparel, travel and online shopping. This app is able to extract relevant entities such as the total sum, store name, single articles and their corresponding prices, and provide a categorization of both the receipt and each article. Suppose you were using this app to earn cash back. You need to take pictures of your receipts and upload them to this app. Please try to answer the following questions.

Finance App prompt: Suppose there is a budgeting application for smartphones that allows for tracking expenses by taking pictures of receipts. This app is able to extract relevant entities such as the total sum, store name, single articles and their corresponding prices, and provide a categorization of both the receipt and each article. Suppose you were using this app to track your expenses. You need to take pictures of your receipts and upload them to this app. Please try to answer the following questions.

AQ2-1. After uploading your receipts, a receipt scanning app may extract information from the receipts. Do you believe that the information is extracted by the app itself locally on your phone instead of transmitting receipts to remote servers for information extraction?

- Yes ○ No ○ Other (please specify)

AQ2-2. I believe that the receipt information is extracted within the app instead of third parties (e.g., other apps, online platforms, service providers).

- Strongly agree
○ Somewhat agree
○ Neither agree nor disagree
○ Somewhat disagree
○ Strongly disagree

AQ2-3. My receipts will **not** be shared to other parties (e.g., other apps, online platforms, service providers).

- Strongly agree ... ○ Strongly disagree (5-level scale)

AQ2-4. My receipts will **not** be shared to some anonymous individuals.

- Strongly agree ... ○ Strongly disagree (5-level scale)

AQ2-5. Who else besides yourself do you think might be able to access the receipts you uploaded?

AQ3-1 to AQ3-6: These questions are about app users' feeling about having their receipts accessible to anonymous individuals.

The following prompt is common to both RS and NRS app users for providing some context about information extraction in receipt scanning apps.

Receipt scanning apps often extract specific information from the uploaded receipts. While some apps leverage automatic technologies to extract information, other apps may ask help from third parties (e.g., other apps, online platforms, service providers) by transmitting receipts to them. Those third parties may share receipts with many anonymous individuals and recruit some of them to manually transcribe receipts' content. Therefore, your uploaded receipts may be accessed by third parties or anonymous individuals.

AQ3-1. How comfortable would you feel if your uploaded receipts are transmitted to a third party (e.g., other apps, online platforms, service providers) and accessed by anonymous individuals?

- Very comfortable
- Comfortable
- Neither comfortable nor uncomfortable
- Uncomfortable
- Very uncomfortable

AQ3-2. Can you please explain your answer to the question above?

AQ3-3. How comfortable would you feel if a receipt **containing your sensitive information** is transmitted to a third party and accessed by anonymous individuals?

- Very comfortable ... ○ Very uncomfortable (5-level scale)

AQ3-4. Can you please explain your answer to the question above?

AQ3-5. How comfortable would you feel if the following information were present on the receipt and visible to anonymous individuals? (Please note that you are the customer.)

- Very comfortable ... ○ Very uncomfortable (5-level scale)

For each of the following pieces of information:

- Customer's name
- Customer's phone number
- Customer's home address
- Customer's email address
- Credit card number's last four digits
- Customer's membership ID
- Sensitive shopping items
- Store's name
- Store's physical address
- Store's phone number
- Store's email address
- Store employee's name
- Date and time information

AQ3-6. Can you explain some of your choices to the above question? If there is any other information on the receipt that you may consider sensitive other than the above mentioned information, please describe them briefly.

AQ4-1 to AQ4-5: These questions are about participants' opinions on who should be responsible for keeping sensitive receipt information protected.

AQ4-1. Protecting the privacy of **customers** (i.e., your privacy) on receipts is important.

- Strongly agree ... ○ Strongly disagree (5-level scale)

AQ4-2. Protecting the privacy of **vendors** on receipts is important.

- Strongly agree ... ○ Strongly disagree (5-level scale)

AQ4-3. Someone has shared your receipts with other parties or anonymous individuals. Do you expect that **the app itself** would obscure your sensitive information (e.g., your name, home

address, phone number, email address, credit card number, membership ID) on the receipts before transmitting your receipts to other parties?

- ☐ Yes ☐ No ☐ Other (please specify)

AQ4-4. Do you expect that **other parties** would obscure your sensitive information before showing your receipts to anonymous individuals?

- ☐ Yes ☐ No ☐ Other (please specify)

AQ4-5. Would you try obscuring some sensitive information from certain people or organizations before uploading your receipts?

- ☐ Yes ☐ No ☐ Other (please specify)

This is an attention check question displayed somewhere in the middle of the survey. It is common to both RS app users and NRS app users.

To help us monitor the quality of our data, please select “Somewhat disagree” from the choices below.

- ☐ Strongly agree ... ☐ Strongly disagree (5-level scale)

AQ5-1 to AQ5-3: These are demographic questions common to both the RS app users and NRS app users.

AQ5-1. What is your gender?

- ☐ Female
- ☐ Male
- ☐ Prefer not to say
- ☐ Other (please specify)

AQ5-2. What is your age group?

- ☐ 18-24 years
- ☐ 25-39 years
- ☐ 40-60 years
- ☐ 61 years or above

AQ5-3. What is the highest degree you have earned?

- ☐ No high school degree
- ☐ High school degree
- ☐ College degree
- ☐ Associate’s degree
- ☐ Bachelor’s degree
- ☐ Master’s degree
- ☐ Doctorate degree
- ☐ Medical degree
- ☐ Prefer not to answer
- ☐ Other (please specify)

This question is at the end of the survey for collecting additional comments.
Other comments or concerns about this survey?

A.2 Summary of Demographics and App Usage

Table 3 summarizes the demographics of RS and NRS app users, and the usage of receipt scanning apps by RS app users.

Table 3. Demographics of RS and NRS App Users, and Usage of Receipt Scanning Apps by RS App Users.

	RS App Users (56)	NRS App Users (52)		RS App Users (56)
Age			Usage Time	
18-24	27(48.2%)	13(25.0%)	Couple of months	3(5.4%)
25-39	17(30.4%)	27(51.9%)	Less than 1 year	10(17.9%)
40-60	12(21.4)	10(19.2%)	Around 1 year	11(19.6%)
60 or older	0(0.0%)	2(3.8%)	More than 1 year	32(57.1%)
Gender			Usage Frequency	
Male	25(44.6%)	26(50.0%)	More than once a day	5(8.9%)
Female	29(51.8%)	26(50.0%)	Once a day	0(0.0%)
non-binary	2(3.6%)	0(0.0%)	More than once a week	23(41.1%)
Read Privacy Policy			Once a week	15(26.8%)
Yes	16(28.6%)	-	More than once a month	12(21.4%)
No	37(66.1%)	-	Once a month	1(1.8%)
Other	3(5.4%)	-	More than once a year	0(0.0%)
			Once a year	0(0.0%)

A.3 Screening Survey

This is the screening survey that app users filled out in order to gain eligibility to participate in the follow-up survey presented in Appendix A.1.

Do you live in the United States?

- ☐ Yes ☐ No

Are you 18 years of age or older?

- ☐ Yes ☐ No

Have you ever shared your receipts to some websites or apps? If Yes, please enter the names of the apps below. If No, just enter “No” for this question. Note: Your eligibility does not depend on your answer to this question. (Open text)

This question is an attention check question used to filter out participants.

What color is grass? The fresh, uncut grass, not leaves or hay. Make sure to select purple as an answer so that we know you are paying attention.

- ☐ Green ☐ Purple

This question was also used to filter out low quality responses.

Please use two sentences to describe your favorite movie. (Open text)

B APPENDIX

B.1 Crowd Worker Survey

Participants for this survey were recruited from the Amazon Mechanical Turk (MTurk) and all participants were given the same questions. In this paper, we use the TQ prefix to number the survey questions asked to turkers (i.e., crowd workers on MTurk). With their consent to participate in this survey study, turkers were presented with the following 31 questions. We list them in six sets (i.e., TQ1- to TQ6-) and added notes in bold font before each set to improve the readability of the paper. Demographics related questions are not listed here due to the space limitation, but the results are summarized at the end of this appendix.

TQ1-1 to TQ1-2: These questions ask a participant to extract information from a receipt. We displayed one of our receipts and asked participants to answer the following two questions. Our purpose is for them to recall or become familiar with the terms such as customer and vendor.

TQ1-1. Please indicate if the receipt shown above contains some type of information of the **customer** (i.e., the receipt owner who had the transaction) by selecting all options that apply:

- ☐ Customer's name
- ☐ Customer's phone number
- ☐ Customer's home address
- ☐ Customer's email address
- ☐ Credit card number's last four digits
- ☐ Customer's membership ID
- ☐ Sensitive shopping items
- ☐ Other (please specify)

TQ1-2. Please indicate if any receipt shown above contains some type of information of a **vendor** (i.e., the store or business with which the customer had the transaction) by selecting all options that apply:

- ☐ Store's name
- ☐ Store's physical address
- ☐ Store's phone number
- ☐ Store's email address
- ☐ Store employee's name
- ☐ Date and time information
- ☐ Other (please specify)

TQ2-1 to TQ2-5: These questions ask participants to consider which types of information may be sensitive on a receipt and how often they see tasks with such information on crowdsourcing platforms.

TQ2-1. Which of the following information on a receipt do you consider as sensitive? Please select all that apply.

- ☐ Customer's name
- ☐ Customer's phone number
- ☐ Customer's home address
- ☐ Customer's email address
- ☐ Credit card number's last four digits
- ☐ Customer's membership ID
- ☐ Sensitive shopping items

- ☐ Store's name
- ☐ Store's physical address
- ☐ Store's phone number
- ☐ Store's email address
- ☐ Store employee's name
- ☐ Date and time information
- ☐ Other (please specify)

TQ2-2. Have you ever seen the following information in receipt transcription tasks before? Please select all that apply.

- ☐ Customer's name ... ☐ Other (same as TQ2-1)

TQ2-3. Regarding the sensitive information you identified above, please indicate how often you work on receipt transcription tasks that contain such sensitive information of other people (i.e., customers or vendors) **on MTurk**.

- ☐ Daily
- ☐ Weekly
- ☐ Monthly
- ☐ Yearly
- ☐ Never
- ☐ Other (please specify)

TQ2-4. Regarding the sensitive information you identified above, please indicate how often you work on receipt transcription tasks that contain such sensitive information of other people (i.e., customers or vendors) **on other crowdsourcing platforms**.

- ☐ Daily ... ☐ Other (same as TQ2-3)

TQ2-5. Regarding your answer to the above question, what other crowdsourcing platforms have you worked on?

TQ3-1 to TQ3-5: These questions are about participants' experiences with transcription tasks on crowdsourcing platforms.

TQ3-1. How many receipt transcription tasks on average do you perform per week on MTurk?

- ☐ Less than 10 HITs per week
- ☐ 10~49 HITs per week
- ☐ 50~99 HITs per week
- ☐ 100~199 HITs per week
- ☐ Greater than 199 HITs per week
- ☐ None
- ☐ Other (please specify)

TQ3-2. Do you like to work on receipt transcription tasks? Please explain why or why not.

TQ3-3. Have you ever seen other types of transcription tasks that contain sensitive information of other people? Please list all that apply.

- ☐ Invoice Transcription
- ☐ Court Document Transcription
- ☐ Financial Document Transcription
- ☐ Business Card Transcription
- ☐ Resume Transcription
- ☐ Other (please specify)

TQ3-4. What are important considerations you take into account if you upload your receipts to some websites or apps?

- ☐ I never upload my receipts

- Satisfactory compensation (rewards)
- Websites or apps are trustworthy
- I upload receipts for financial management
- Proper privacy protection (e.g., the sensitive information will be obscured)
- Other (please specify)

TQ3-5. In addition to transcription tasks, have you ever seen other tasks that contain sensitive information of other people? If yes, please briefly describe the task(s), the type(s) of sensitive information, and the name(s) of the crowdsourcing platform(s).

TQ4-1 to TQ4-9: These questions are about workers' attitudes towards privacy on MTurk.

TQ4-1. Protecting the privacy of **customers** on receipts is important.

- Strongly agree
- Somewhat agree
- Neither agree nor disagree
- Somewhat disagree
- Strongly disagree

TQ4-2. Protecting the privacy of **vendors** on receipts is important.

- Strongly agree ... ◦ Strongly disagree (5-level scale)

TQ4-3. Who do you think should be responsible for protecting other people's sensitive information on receipts? Please select all that apply.

- ☐ Requesters
- ☐ MTurk
- ☐ Customers
- ☐ Vendors
- ☐ Other (please specify)

TQ4-4. How comfortable do you feel about working on receipt transcription tasks that contain a **customer's** sensitive information?

- Very comfortable
- Comfortable
- Neither comfortable nor uncomfortable
- Uncomfortable
- Very uncomfortable

TQ4-5. Can you please explain your answer to the question above? Please write down at least two sentences.

TQ4-6. How comfortable do you feel about working on receipt transcription tasks that contain a **vendor's** sensitive information?

- Very comfortable ... ◦ Very uncomfortable (5-level scale)

TQ4-7. Can you please explain your answer to the question above? Please write down at least two sentences.

TQ4-8. How comfortable would you feel about having your receipts that contain **your** sensitive information transcribed by other MTurk workers?

- Very comfortable ... ◦ Very uncomfortable (5-level scale)

TQ4-9. Can you please explain your answer to the question above? Please write down at least two sentences.

TQ5-1 to TQ5-3: These questions are about crowd workers' opinions on the requesters' task purposes, identities, and receipt sources.

TQ5-1. In your opinion (or experience), how will requesters use your receipt transcription results? Please also explain your answer.

TQ5-2. In your opinion (or experience), who are the requesters that post receipt transcription tasks? Please also explain your answer.

TQ5-3. In your opinion (or experience), how did those requesters obtain those receipts? Please also explain your answer.

This is an attention check question displayed somewhere in the middle of the survey. To help us monitor the quality of our data, please select “Somewhat disagree” from the choices below.

☐ Strongly agree ... ☐ Strongly disagree (5-level scale)

TQ6-1 to TQ6-6: These are the demographics questions we asked workers.

TQ6-1. What is your gender?

- ☐ Female
- ☐ Male
- ☐ Prefer not to say
- ☐ Other (please specify)

TQ6-2. What is your age group?

- ☐ Under 18 years old
- ☐ 18-24 years
- ☐ 25-39 years
- ☐ 40-49 years
- ☐ 50-59 years
- ☐ 6 years or above

TQ6-3. Does MTurk provide primary or supplementary income to you?

- ☐ Primary
- ☐ Supplementary

TQ6-4. What is the highest degree you have earned?

- ☐ No high school degree
- ☐ High school degree
- ☐ Some college
- ☐ Associate's degree
- ☐ Bachelor's degree
- ☐ Master's degree
- ☐ Doctorate degree
- ☐ Medical degree
- ☐ Prefer not to answer

TQ6-5. How much time do you spend on MTurk?

- ☐ Less than 10 hour per week
- ☐ 10~20 hours per week
- ☐ 20~30 hours per week
- ☐ 30~40 hours per week
- ☐ More than 40 hours per week

TQ6-6. How many years or months of experience do you have with working on MTurk?

- ☐ Less than 1 month
- ☐ 1~3 months
- ☐ 3~6 months

- 6~12 months
- 1~3 years
- 3~6 years
- More than 6 years
- Other (please specify)

This question is at the end of the survey for collecting additional comments.
Other comments or concerns about this survey?

B.2 Summary of Demographics and Worker Experiences on MTurk

Table 4 summarizes the demographics of crowd workers and their general experiences on MTurk.

Table 4. Demographics and Work Experiences of Crowd Workers.

Crowd Workers (102)		Crowd Workers (102)	
Age		Work Experience	
18-24	1(1.0%)	1-3 months	7(6.9%)
25-39	74(72.5%)	3-6 months	2(2.0%)
40-49	17(16.7%)	6-12 months	6(5.9%)
50-59	6(5.9%)	1-3 years	36(35.3%)
60 or older	4(3.9%)	3-6 years	32(31.4%)
Gender		> 6 years	19(18.6%)
Male	64(62.7%)	Work Time/Week	
Female	38(37.3%)	< 10 hrs/week	10(9.8%)
MTurk Income Source		10-20 hrs/week	43(42.2%)
Primary	19(18.6%)	20-30 hrs/week	27(26.5%)
Supplementary	83(81.4%)	30-40 hrs/week	14(13.7%)
		> 40 hrs/week	8(7.8%)

C APPENDIX

C.1 The 14 RS Apps and Their Analysis

Table 5 presents the basic information, privacy policy analysis, and network traffic analysis of 14 major RS apps (11 are what we identified for AQ1-3 and three are what RS app users further specified for AQ1-3). Our privacy policy and network traffic analyses focused on the data transferring, sharing, and processing practices of these apps. In terms of privacy policies, all 14 apps contained sharing practices and somehow mentioned the entities with whom the collected users’ data such as receipts would be shared. Specifically, all apps except for Amazon Shopper Panel indicated that they would share the collected data with third parties such as other service providers. However, five apps did not provide any information about the data processing practices; only four of the remaining nine apps explicitly mentioned who may process users’ data such as receipts. Meanwhile, we used the VPN-based PCAPdroid network monitor [51] to analyze the network traffic. We found that most (12 out of 14) apps have large payloads transferred to remote servers whenever we use their in-app camera function to take a photo of a receipt of ours, which indicates that they do send receipt images to remote servers for processing. We do not have the results for the remaining two apps as they reported server errors when PCAPdroid was running.

C.2 Inter-coder Reliability and Codebook

Table 6 lists the inter-coder reliability Krippendorff’s α coefficient for each open-ended question. Table 7 and Table 8 list the codes with frequency for the app user study and the crowd worker study,

Table 5. Privacy Policy Analysis and Behavior Analysis of 14 Major Receipt Scanning Apps. (*: Identified by us as an option for AQ1-3, #: Specified by RS app users for AQ1-3)

App Name	App Type	# of Downloads Reported on Google Play Store	Percentage of RS App Users Who Selected or Mentioned App in AQ1-3	Privacy Policy Analysis				Behavior Analysis	
				Contain Sharing Practice	Shared with Whom	Contain Processing Practice	Processed by Whom	Large Payloads Transfer	Transfer Destination
Ibotta*	Rewards	10,000,000+	67.9%	Yes	Third Parties	No	N/A	Yes	Amazon Server
Receipt Pal*	Rewards	1,000,000+	42.9%	Yes	Employees, Internal Entities, Third Parties	Yes	Third Parties	Yes	NPD Group Server
Fetch Rewards*	Rewards	10,000,000+	37.5%	Yes	Third Parties	Yes	Not Mentioned	Yes	Amazon Server
Receipt Hog*	Rewards	1,000,000+	26.8%	Yes	Third Parties	No	N/A	Yes	Amazon Server
CoinOut*	Rewards	1,000,000+	23.2%	Yes	Employees, Internal Entities, Third Parties	Yes	Not Mentioned	Yes	Amazon Server
Expensify*	Finance	1,000,000+	14.3%	Yes	Third Parties	Yes	Not Mentioned	Yes	CloudFlare Server
Receipt Bank (Dext)*	Finance	100,000+	12.5%	Yes	Third Parties	Yes	Internal Entities	Yes	Amazon Server
Shopkick*	Rewards	10,000,000+	12.5%	Yes	Third Parties	No	N/A	-	-
Quickbooks*	Finance	5,000,000+	8.9%	Yes	Third Parties	Yes	Not Mentioned	Yes	Amazon Server
Smart Receipts*	Finance	500,000+	8.9%	Yes	Employees, Internal Entities, Third Parties	Yes	Employees, Internal Entities, Third Parties	Yes	Amazon Server
Amazon Shopper Panel#	Rewards	100,000+	7.1%	Yes	Not with Third Parties	Yes	Amazon Reviewers	Yes	Amazon Server
Zoho Expense*	Finance	100,000+	5.4%	Yes	Employees, Internal Entities, Third Parties	No	N/A	Yes	Zoho Server
Coupons.com#	Rewards	5,000,000+	3.6%	Yes	Third Parties	No	N/A	-	-
Checkout 51#	Rewards	10,000,000+	1.8%	Yes	Employees, Third Parties	Yes	Not Mentioned	Yes	Amazon Server

respectively. Each code category reflects a particular open-ended question for the participants in each study. For example, if an app user answered AQ1-2 with earning cashback as the reason for using RS apps, the code is “Cashback_Saving” (*code_id* is 1) in the code category “AQ1-2: Reason_on_Using_RS_App” (Table 7).

Table 6. Inter-coder Reliability (Krippendorff’s α Coefficient) for Each Open-ended Question.

Survey Study	Question	α
App User (RS)	AQ1-2: Reason_on_Using_RS_App	0.95
	AQ2-5: Who_May_Access_Uploaded_Receipts	0.87
	AQ3-2: Comfort_on_Transmit_Access_Receipt	0.92
	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	0.80
App User (NRS)	AQ1-2: Reason_on_Not_Using_RS_App	0.83
	AQ2-5: Who_May_Access_Uploaded_Receipts	0.95
	AQ3-2: Comfort_on_Transmit_Access_Receipt	0.75
	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	0.80
Crowd Worker	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	0.92
	TQ4-5: Comfort_on_Tasks_with_Customer’s_Info	0.72
	TQ4-7: Comfort_on_Tasks_with_Vendor’s_Info	0.86
	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	0.85
	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	0.91
	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	0.92
	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	0.87

Received July 2022; revised January 2023; accepted March 2023

Table 7. Final Codebook with Code Frequency (i.e., the number of responses with the corresponding code)
Part 1 – the App User Study. The word “Other” in the codes represents invalid or irrelevant responses.

User Type	code_id	code_category	code	freq.
RS App Users	1	AQ1-2: Reason_on_Using_RS_App	Cashback_Saving	44
	2	AQ1-2: Reason_on_Using_RS_App	Positive_Usage_Experience	5
	3	AQ1-2: Reason_on_Using_RS_App	Receipt_Management	6
	4	AQ1-2: Reason_on_Using_RS_App	Other	1
	5	AQ2-5: Who_May_Access_Uploaded_Receipts	App_Itself	26
	6	AQ2-5: Who_May_Access_Uploaded_Receipts	Only_Receipt_Owner	6
	7	AQ2-5: Who_May_Access_Uploaded_Receipts	Third_Parties	17
	8	AQ2-5: Who_May_Access_Uploaded_Receipts	No_Idea	3
	9	AQ2-5: Who_May_Access_Uploaded_Receipts	Other	4
	10	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Privacy_Concern	15
	11	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Potential_Risks	9
	12	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Lack_of_Transparency_or_Accountability	2
	13	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Other	1
	14	AQ3-2: Comfort_on_Transmit_Access_Receipt	Neutral->Information_Limited_or_Trivial	6
	15	AQ3-2: Comfort_on_Transmit_Access_Receipt	Neutral->Rewards_Outweigh_Risks	2
	16	AQ3-2: Comfort_on_Transmit_Access_Receipt	Neutral->Other	6
	17	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->Information_Limited_or_Trivial	5
	18	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->Rewards_Outweigh_Risks	4
	19	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->No_Concern	2
	20	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->Other	4
	21	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Need_to_Protect_Sensitive_Info	5
	22	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Privacy_Concern	19
	23	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Potential_Risks	15
	24	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Lack_of_Transparency_or_Accountability	4
	25	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Other	2
	26	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Neutral->Depends_on_Info	2
	27	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Neutral->Information_Limited_or_Trivial	1
	28	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Neutral->Adopted_Privacy_Protection	1
	29	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Neutral->Other	3
	30	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Comfortable->Adopted_Privacy_Protection	1
	31	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Comfortable->Rewards_Outweigh_Risks	2
	32	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Comfortable->Information_Limited_or_Trivial	1
NRS App Users	33	AQ1-2: Reason_on_Not_Using_RS_App	Privacy_Concern	10
	34	AQ1-2: Reason_on_Not_Using_RS_App	Interested_in_But_Didn't_Use_Apps_Yet	2
	35	AQ1-2: Reason_on_Not_Using_RS_App	Unaware_or_Unfamiliar_With_Apps	8
	36	AQ1-2: Reason_on_Not_Using_RS_App	Lack_of_Transparency_or_Accountability	3
	37	AQ1-2: Reason_on_Not_Using_RS_App	Potential_Risks	4
	38	AQ1-2: Reason_on_Not_Using_RS_App	App_Usage->Inconvenient	4
	39	AQ1-2: Reason_on_Not_Using_RS_App	App_Usage->Using_Other_Tools	4
	40	AQ1-2: Reason_on_Not_Using_RS_App	App_Usage->Unknown_Benefit	8
	41	AQ1-2: Reason_on_Not_Using_RS_App	Other	9
	42	AQ2-5: Who_May_Access_Uploaded_Receipts	App_Itself	19
	43	AQ2-5: Who_May_Access_Uploaded_Receipts	Only_Receipt_Owner	8
	44	AQ2-5: Who_May_Access_Uploaded_Receipts	Third_Parties	16
	45	AQ2-5: Who_May_Access_Uploaded_Receipts	Malicious_Entity	3
	46	AQ2-5: Who_May_Access_Uploaded_Receipts	Other	6
	47	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Privacy_Concern	10
	48	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Unwilling_to_Share	13
	49	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Potential_Risks	8
	50	AQ3-2: Comfort_on_Transmit_Access_Receipt	Uncomfortable->Lack_of_Transparency_or_Accountability	3
	51	AQ3-2: Comfort_on_Transmit_Access_Receipt	Neutral->Depends_on_Info	8
	52	AQ3-2: Comfort_on_Transmit_Access_Receipt	Neutral->Information_Limited_or_Trivial	1
	53	AQ3-2: Comfort_on_Transmit_Access_Receipt	Neutral->Other	6
	54	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->Adopted_Privacy_Protection	1
	55	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->Information_Limited_or_Trivial	1
	56	AQ3-2: Comfort_on_Transmit_Access_Receipt	Comfortable->No_Concern	1
	57	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Privacy_Concern	10
	58	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Unwilling_to_Share	9
	59	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Depends_on_Info	3
	60	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Potential_Risks	21
	61	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Uncomfortable->Lack_of_Transparency_or_Accountability	5
	62	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Neutral->Privacy_Concern	1
	63	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Neutral->Never_Thought_about_It	1
	64	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Comfortable->Information_Limited_or_Trivial	1
	65	AQ3-4: Comfort_on_Transmit_Access_Receipt_with_Sensitive_Info	Comfortable->Other	1

Table 8. Final Codebook with Code Frequency (i.e., the number of responses with the corresponding code)
 Part 2 – the Crowd Worker Study. The word “Other” in the codes represents invalid or irrelevant responses.
 (RT: Receipt Transcription)

code_id	code_category	code	freq.
66	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Not_Like->Underpaid	53
67	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Like->Easy	15
68	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Not_Like->Time_Consuming	7
69	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Like->Entertaining	8
70	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Other	5
71	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Depends_on_Tasks	10
72	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Not_Like->Lack_of_Experience	2
73	TQ3-2: Like_to_Work_on_RT_Tasks_or_Not_and_Reason	Not_Like->Lack_of_Interest	2
74	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Uncomfortable->Respect_Others'_Privacy	19
75	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Uncomfortable->Lack_of_Transparency_or_Accountability	5
76	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Uncomfortable->Unclear_Customer_Consent	3
77	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Uncomfortable->Afraid_of_Being_Blamed_for_Incident	4
78	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Uncomfortable->Potential_Risks	5
79	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Uncomfortable->Other	3
80	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Neutral->Merely_Focus_on_Tasks	5
81	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Neutral->Consider_Themselves_Trustworthy	7
82	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Neutral->Not_Responsible_for_Customer's_Privacy	3
83	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Neutral->Depends_on_Info	3
84	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Neutral->Other	1
85	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Comfortable->Consider_Themselves_Trustworthy	18
86	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Comfortable->Assume_Customer_Consented	6
87	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Comfortable->Merely_Focus_on_Tasks	12
88	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Comfortable->Not_Responsible_for_Customer's_Privacy	5
89	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Comfortable->Information_Limited_or_Trivial	2
90	TQ4-5: Comfort_on_Tasks_with_Customer's_Info	Comfortable->Other	1
91	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Uncomfortable->Respect_Vendors'_Privacy	3
92	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Uncomfortable->Lack_of_Transparency_or_Accountability	1
93	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Uncomfortable->Afraid_of_Being_Blamed_for_Incident	1
94	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Uncomfortable->Other	3
95	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Neutral->Public_Information	8
96	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Neutral->Depends_on_Info	3
97	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Neutral->Vendor's_Decision_on_Their_Info_on_Receipts	1
98	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Neutral->Other	2
99	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->Public_Information	50
100	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->No_Concern	6
101	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->Not_Responsible_for_Vendor's_Privacy	4
102	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->Merely_Focused_on_Tasks	4
103	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->Depends_on_Info	4
104	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->Vendor's_Decision_on_Their_Info_on_Receipts	9
105	TQ4-7: Comfort_on_Tasks_with_Vendor's_Info	Comfortable->Other	3
106	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Uncomfortable->Lack_of_Transparency_or_Accountability	5
107	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Uncomfortable->Unwilling_to_Share	16
108	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Uncomfortable->Privacy_Concern	26
109	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Uncomfortable->Lack_of_Trust_on_Others	19
110	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Uncomfortable->Potential_Risks	15
111	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Uncomfortable->Other	3
112	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Neutral->Merely_Focused_on_Tasks	1
113	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Neutral->Depends_on_Info	3
114	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Neutral->Trust_Others	1
115	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Neutral->Adopted_Privacy_Protection	1
116	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Comfortable->Trust_Others	3
117	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Comfortable->Their_Own_Decision	2
118	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Comfortable->Depends_on_Info	3
119	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Comfortable->Information_Limited_or_Trivial	3
120	TQ4-9: Comfort_on_Having_Their_Receipts_Transcribed_by_Others	Comfortable->Other	1
121	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Train_AI_Models	10
122	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Market_Exploration	27
123	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Malicious_Purpose	4
124	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Information_Verification	19
125	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Research_Purpose	6
126	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	No_Idea	14
127	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Receipt_Management	16
128	TQ5-1: Opinion_on_How_Requesters_May_Use_Info_on_Receipts	Other	6
129	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	AI_Model_Developers	4
130	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Researchers_in_Colleges_Universities	6
131	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Receipt_Scanning_App_Providers	14
132	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Data_Analytic_Companies	12
133	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Market_Exploration_Companies	10
134	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Named_Task_Requesters	17
135	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Vendor_or_Brand_Affiliations	9
136	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	No_Idea	17
137	TQ5-2: Opinion_on_Who_are_Requesters_of_RT_Tasks	Other	13
138	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	From_Vendor_or_Brand_Affiliations	14
139	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	From_Crowdsourcing_Tasks	9
140	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	From_Receipt_Scanning_App_Providers	30
141	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	From_Online_Services	6
142	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	From_Customers_or_Their_Discarded_Receipts	17
143	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	From_Reward_Programs	11
144	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	No_Idea	10
145	TQ5-3: Opinion_on_How_Requesters_Obtained_Receipts	Other	5