Emerging Privacy Issues and Solutions in Cyber-Enabled Sharing Services

KE YAN, China Jiliang University
WEN SHEN, University of California, Irvine
HUIJUAN LU, China Jiliang University
QUN JIN*, China Jiliang University, Waseda University

Fast development of sharing services becomes a crucial part of the process in constructing a cyber-enabled world, as sharing services reinvent how people exchange and obtain goods or services. However, privacy leakage or disclosure is a key concern which may hinder the development of sharing services. While significant efforts have been undertaken to address various privacy issues in recent years, there is a surprising lack of a review for privacy concerns in the cyber-enabled sharing world. To bridge the gap, in this study, we survey and evaluate existing and emerging privacy issues relating to sharing services from various perspectives. Differing from existing similar works on surveying sharing practices in various fields, our work comprehensively covers six directions of sharing services in the cyber-enabled world, and selects solutions mostly from the recent five years. Finally, we conclude the issues and solutions from three perspectives, namely, the user, platform and service provider perspectives.

Keywords: Cyber Technology, Sharing Service, Privacy, Crowdsourcing, Collaborative Consumption

1 INTRODUCTION

Cyberization is transforming our physical living world into a virtual computerized world by leveraging the Internet and computational methodologies [88, 89]. In the virtual computerized world, or more specifically, the cyber-enabled world, people are connected via Internet regardless of physical distances. Cyber-enabled sharing services, or in short, sharing services, which provide information, goods, and services in a shared form to multiple individuals, who know or do not know each other, are essential and necessary components of cyber-world development and probably the most exciting cyber-related concept in the current stage of cyberization. Sharing services encourage people to share both virtual and physical assets through the Internet using cyber-enabled clients, including mobile phones, all kinds of computers and similar digital devices. Sharing services contribute to the fast development of cyber technology, where the control, responsibility for the common good, earnings, capitalization, information, and efforts are all shared among the participants or distributed to peer members [121]. In recent years, cyberized sharing service companies, such as Uber, Airbnb, Etsy and Amazon Family Library, have been overwhelmingly popular and enjoyed incredible growth [13, 101, 153].

There are various reasons for people to participate in sharing practices. For instance, no single entity or person can control the whole market or economy, although some participants have more regulatory power than others. All participants share the responsibility of making the market to operate healthily. This form of collaborative economy or peer-to-peer (P2P) sharing leads to more efficient resource allocations and more sustainable lifestyles. However, for any participant in the sharing practice, regardless of whether he/she is a user or service provider, all the other people who are involved in the same sharing practice can be potential

*Corresponding author: Qun Jin (Email address: jin@waseda.jp).
This work is supported by the National Natural Science Foundation of China, under grant 61602431.
Author's addresses: K. Yan, H. Lu and Q. Jin, College of Information Engineering, China Jiliang University, 258 Xueyuan Street, Hangzhou, China, 310018, emails: yanke@cjlu.edu.cn, keddiyan@gmail.com (K. Yan) and hjlu@cjlu.edu.cn (H. Lu); W. Shen, Department of Informatics, University of California Irvine, Irvine, CA 92697, email: wen.shen@uci.edu; Q. Jin, Department of Human Informatics and Cognitive Sciences, Waseda University, 2-579-15 Mikajima, Tokorozawa, 359-1192, Japan.

attackers who compromise his/her privacy. Moreover, to attract more people to share, it is necessary to build trust, establish reputation, protect privacy and guarantee security for both the user and service provider [15]. Personal privacy concern is the main factor that hinders the development of sharing services in the cyber-enabled world [39, 43]. On one hand, people are reluctant to adopt sharing practices because of the concerns about privacy disclosure [47, 52, 82]; on the other hand, sharing service providers insist that personal data is part of the necessary information in user experience analysis for improving service quality. While only privacy protection is explored in this paper, the authors would like to note that privacy is relevant and closely related to trust, reputation and security. Users need to trust the service provider, which implies that the service provider must have a good reputation that the users can trust. Reputations are established through the interactions between the users and service providers. However, during the interaction process, privacy issues arise because pieces of private information from both parties are inevitably revealed to each other.

Unfortunately, due to the fast development pace of sharing service technology, privacy issues were not well addressed before sharing services were widely spread over the physical world [71]. Cyber-technologies that can be used to protect various aspects of privacy are urgently desired to prohibit both the user and service provider from revealing each other's sensitive information. In the starting stage of the sharing economy, some service providers may intentionally neglect the privacy issues to survive in the highly competitive business environment. In other words, profit is usually the highest priority for most starter-level sharing service companies. In this study, we surveyed over one hundred research works from the past five years that are closely related to the privacy issues with the newly developed sharing service technologies and observed that the privacy protection level is highly related to the number of users who participate the sharing service, which affects the final profit of the service providers. In addition, from the user's perspective, increasing the self-awareness of privacy disclosure is an important task for the users to protect themselves in the current stage of cyberization.

In summary, the emerging privacy issues of sharing services in the cyber-enabled world and the available solutions are reviewed comprehensively. From the literature, we summarize the sharing services in the current stage of the cyber-enabled world into two categories [21, 121]:

- **Crowdsourcing** employs collective intelligence or power to fulfil tasks or achieve goals. Concrete examples of crowdsourcing are Internet crowdsourcing marketplaces, crowdfunding, and crowdtesting [40]. For a typical crowdsourcing practice, there are, in general, three roles involved: the task requester, the platform and the worker. The task requester posts tasks on the platform and attracts workers to finish the job in a crowdsourcing way.
- **Collaborative consumption** allows consumers to use products or services without full ownership. Concrete examples of collaborative consumption include collaborative online shopping, ridesharing, and homesharing practices [13]. For a typical collaborative consumption model, there are again three roles involved: the host, the platform and the customer. Differing from the crowdsourcing practice, the host provides P2P sharing of goods or services to customers through an online platform. In this study, we refer to the combination of task requesters and hosts as service providers, and the combination of workers and customers as users.

The review of privacy issues and solutions follows the above two outlines and reveals the main concerns in the literature, which include the requester's data protection, the balance between privacy protection and sacrifice, data encryption, unreliable data analysis, location privacy and physical privacy. Figure 1 lists a taxonomy of important works that are surveyed for privacy issues and solutions in crowdsourcing and collaborative consumption practices.

Although there are similar works concerning privacy in sharing practices from the literature, e.g., [2, 8, 48, 59, 116], they focused on traditional privacy protection methods. Traditional privacy protection techniques, including k-anonymity [119, 130], l-diversity [90] and t-closeness [80], have been heavily reviewed in the past

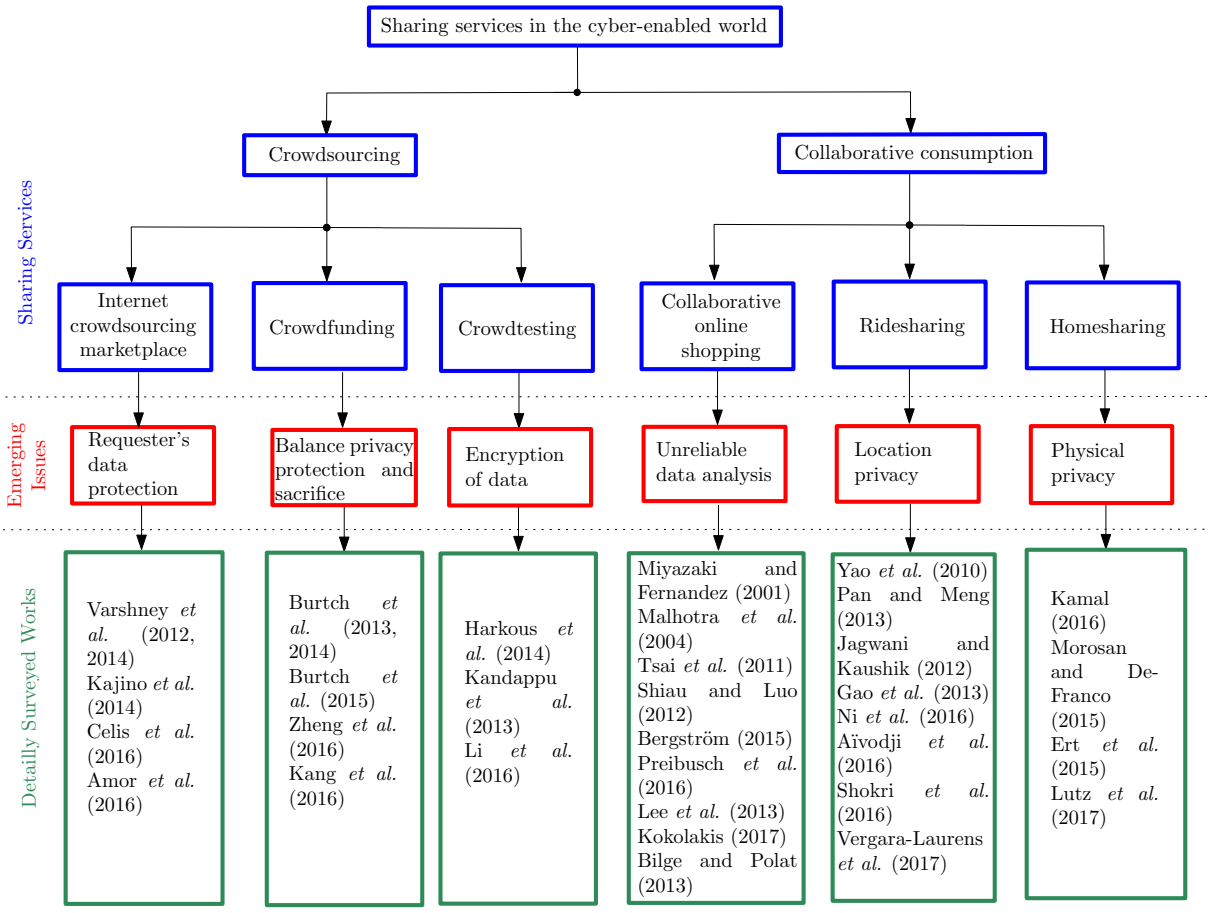

Fig. 1. Taxonomy of sharing services in the cyber-enabled world following the categorization of crowdsourcing and collaborative consumption practices (in blue rectangles), with identified emerging privacy issues (in red rectangles) and surveyed works in the literature (in green rectangles).

few decades. In contrast, our work focuses on privacy protection technique development in the past five years, skips the traditional approaches and covers technologies comprehensively in the area of cyber-enabled sharing services. Most surveyed works in this study were published in the years ranging from 2013 to 2016. The sources of the reviewed papers include the most popular databases, such as ACM Digital Library, IEEE Xplore Digital Library, Springer Link, ScienceDirect and Google Scholar. The searched keywords include 'sharing service', 'privacy issue', 'privacy protection', 'crowdsourcing privacy', 'collaborative consumption privacy', 'crowdfunding privacy' and etc.

This survey work is organized as follows: The emerging privacy issues and solutions of crowdsourcing are analyzed in Section 2. The emerging privacy issues and solutions of collaborative consumption are reviewed in Section 3. In Section 4, we summarize all the privacy issues in Sections 2 and 3 from the user, platform and service provider perspectives. In Section 5, several conclusions are drawn regarding cyber technology development to predict the future trends in the development of cyber-enabled sharing technologies.

2 PRIVACY ISSUES AND SOLUTIONS IN CROWDSOURCING PRACTICES

Crowdsourcing refers to the distribution of tasks that cannot be easily accomplished in a traditional way to a large group of online workers [62] (Figure 2). The tasks are usually difficult problems or issues that cannot easily be resolved by small groups of users or individuals. Despite its many advantages, crowdsourcing brings increased risks of information leakage and privacy violation, which limits its development and application potential.

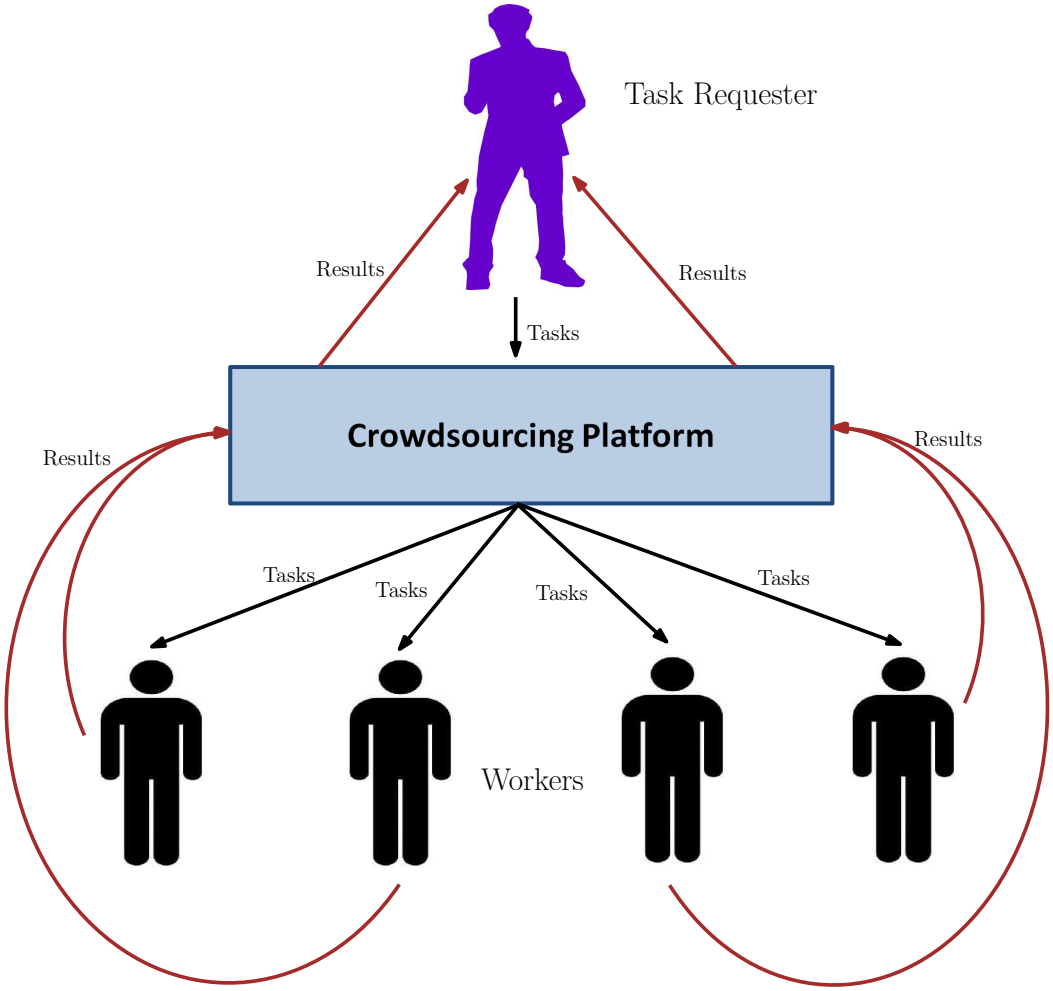

Fig. 2. The crowdsouring practice consists of types of users: task requester and the workers. The task requester distributes tasks to the workers through the platform, and collects the feedbacks from the workers in a reverse way.

There are two types of users in a crowdsourcing platform: the worker (or the employee) and the task requester (or the employer). The task requester provides incentives and tasks, while the worker performs the tasks to receive the incentives. The interaction between them gives rise to the risks of information leakage and privacy violation, which might be either unidirectional or bidirectional. In other words, either the worker or the requester, or both, have the possibility to leak sensitive information or violate the privacy agreement.

We next identify potential privacy leaking risks in three key applications of crowdsourcing: Internet crowdsourcing marketplaces, crowdfunding, and crowdtesting. For each application, we consider the privacy protection issues in the process of sharing practice and survey the existing solutions in the literature.

2.1 Crowdsourcing Marketplace

An online crowdsourcing marketplace provides a platform for matching the task requesters and the task performers for mutual benefits. Numerous crowdsourcing marketplaces have been developed during the past few years, e.g., the Amazon Mechanical Turk (MTurk) [75], which enables individuals and business entities to use their own intelligence to perform tasks that are 'difficult' for automated computerized programs. Requesters post jobs or work in the form of human intelligence tasks on the MTurk platform, while workers browse the tasks and complete them to earn monetary incentives from the requesters.

Data privacy concerns limit the spreading speed of crowdsourcing because many users refuse to participate in crowdsourcing if personal data cannot be not securely protected. For example, when a requester evaluates the design of a particular artefact, it is likely that the requester desires to prevent exposure of the artefact. Similarly, a testing organization usually requires test takers not to disclose the content of the test. However, unlike a testing organization, which has the power to penalize test takers who violate the confidentiality agreement, the requester does not always have the power or effective methods to penalize workers who leak sensitive data or extract information for other purposes. What makes it worse is that the workers are sometimes unreliable and usually not identifiable. Therefore, it is challenging to protect the privacy of the requesters.

Generally, there are two approaches tackling the privacy protection problem for the requesters. The first solution, which is introduced by Varshney, distorts sensitive data directly using random perturbations to conceal private information [136]. A series of extensions were introduced by the same group of researchers for completing the framework based on coding theories [138, 139, 149]. The coding theory successfully hides the sensitive information from the workers. However, it loses the task performance quality when random perturbations are added to the original data. A mathematical model was used to analyze the tradeoffs between privacy, reliability, and cost, by considering five insight elements: error-correcting codes, reliability, perturbation, decoding and collusion attacks [137].

The second approach is the instance clipping protocol (ICP), which was introduced by Little and Sun [84] and Chen *et al.* [33]. Kajino *et al.* [67] proposed a quantitative analysis framework (QAF) based on the instance clipping protocol. The QAF evaluates the instance-privacy preserving protocols and protects the target privacy, which is defined as contextual information. The instance-privacy preserving protocols preserve instance privacy at the cost of task performance. For instance, in Figure 3, a task (represented by a 2D shape) is clipped by clipping windows which are marked by red boxes. Each worker is only allowed to access one clipping window for his/her task result. The ICP preserves privacy but may decrease the quality of the task results. Similar to Varshney's work, there is a tradeoff between privacy preservation and task quality. The instance clipping protocol clips an instance by a moving window, which preserves the data privacy by limiting the data that each worker acquires.

Celis *et al.* [29] improved the clipping protocol by utilizing a collusion network. In the collusion network, the requesting task can be partitioned among different workers with minimal privacy leaks. Moreover, a crowdsourcing framework is proposed with three operations: PULL, PUSH and Tug Of War (TOW). PULL and PUSH are two usual operations that represent a worker choosing tasks and a requester choosing workers, respectively. TOW is an intermediate layer that is built into the system to minimize the information leakage. The TOW operation accounts for the worker's personal information, such as social networks, financial information, and task history. This might lead to information leakage from the worker side.

Amor *et al.* [6] introduced a system called SocialCrowd for managing competition and collaboration in the crowdsourcing process. The SocialCrowd system deeply analyzes the social relationships of the workers and

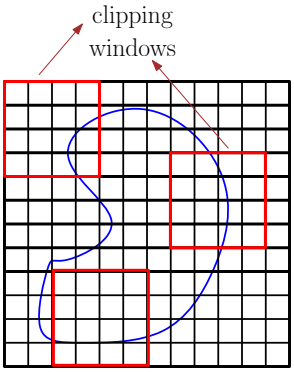

Fig. 3. The instance clipping protocol: a task (represented by a 2D shape), is clipped by clipping windows which are marked by red boxes.

organizes them based on clustering algorithms. Experimental results showed that the data leakage was effectively prevented and the efficiency of the crowdsourcing task was increased. The main concern in Amor *et al.*'s work was the time complexity since the optimal solution could be found only by searching the whole space. One solution that was proposed by the authors was to use a heuristic random search algorithm, which could be risky in terms of becoming trapped in local extremes.

Table 1. References, main objectives, proposed solutions and important insufficiency of the surveyed works for crowdsourcing marketplace.

Reference	**Year**	**Main objective**	**Proposed solution**	**Important insufficiency**
Varshney *et al.* [136, 137]	2012, 2014	Studying the tradeoffs between privacy, reliability, and cost	An improved coding scheme by considering five insight elements	Unable to solve the collision between privacy and task performance quality
Kajino *et al.* [67]	2014	Protecting the requesters' privacy defined as contextual information	Quantitative analysis framework based on instance clipping protocol	Making tradeoff between task performance and privacy
Celis *et al.* [29]	2016	Partitioning the task with minimal privacy leaks	The collusion network	Information leakage from the worker side
Amor *et al.* [6]	2016	Increasing the privacy awareness	SocialCrowd	Using heuristic function for optimal solution search

Table 1 lists all the references that we have discussed in this section, including their main objectives, proposed solutions, and possible weaknesses. In summary, while most recent studies of privacy protection in crowdsourcing marketplaces consider coding schemes or clipping protocols, new technologies, such as SocialCrowd, are proposed to help improve the data security. The common problem for the coding schemes and clipping protocols is that the manipulation of the original data decreases the task performance quality. Moreover, the extra

time complexity that is added to the original data transmission and storage process is a notable issue for those efforts on privacy protection. In addition, while the traditional works focus on protecting the requesters' data in a fundamental way, other issues are raised for improving user awareness of privacy leakage during crowdsourcing practice, which will be discussed in Section 4.1.

2.2 Crowdfunding

Crowdfunding has undergone fast development recently [16, 100]. It enables founders of various ventures to fund their projects by collecting funds or other resources from a large group of individuals through an online platform, such as Kickstarter [77] or Indiegogo [9]. While most works focus on economic aspects of crowdfunding, few address privacy issues [23]. To bridge the gap between privacy concerns and practical use of crowdfunding, in this subsection, we review several existing works on privacy concerns in crowdfunding practices.

In the practice of crowdfunding, a fundraiser (the requester) proposes a project with a plan on an online platform and convinces users or supporters to invest small amounts of money in the project. The modern crowdfunding platforms, such as Indiegogo, allow users to customize their security level and conceal their personal information, such as their name and the amount of their contribution. However, our surveyed works suggest that revealing a certain amount of private information can be helpful in crowdfunding practice. For example, concealing the contribution amount of the prior contributor may discourage followers from contributing more to the crowdfunding project [24]. Moreover, a fundraiser may choose to reveal more of his/her personal information to attract crowdfunders [128].

Burtch *et al.* [24, 25] conducted a series of experiments on a large-scale crowdfunding platform to test the relationship between the security setup and users' willingness to contribute. An econometric model was constructed where the dependent variables included the likelihood of information hiding and contribution amount from crowdfunders. The independent variables included the privacy control of the fundraiser's platform, elapsed time of fundraising, and fundraiser's reputation. Six hypotheses were formulated: the privacy concern effect (H1), exposure effect (H2), extremity effect (H3), self-contribution effect (H4), anchor effect (H5) and censorship effect (H6). The econometric model is shown in Figure 4, where the likelihood of information hiding and the amount of contribution from crowdfunders are affected by the six hypotheses, as shown with arrows. Although the econometric model provided valuable suggestions on privacy protection, it did not consider other factors that may influence the crowdfunders' decisions, such as wording, information regulation, transaction mechanism design and presentation format.

In 2015, Burtch *et al.* [26] conducted another online experiment to study the hidden cost of protecting crowdfunders' privacy by utilizing modern techniques, such as invisible transaction information. Their result indicated that privacy protection increased the net funding in overall, but may decrease the contribution amount from each individual. The main concern of this work is that the experiments were conducted in a randomized pattern. Moreover, the users were given complete freedom for their fund contributions, which made the experimental result unreliable.

Zheng *et al.* [156] analyzed the importance of trust management in the practice of crowdfunding. They constructed a research model to test five hypotheses. Experimental results showed that effective trust management techniques significantly improve the fundraising performance. Moreover, they found that records of prior fundraising success positively promote the entrepreneur-sponsor interaction in crowdfunding practices. However, the study only focused on trust management and ignored other highly influential factors, such as funding information and presentation format in the funding description.

Kang *et al.* [70] proposed a structural equation modeling technique for revealing a fundraiser's true motivation for a crowdfunding investment. They employed three measurement factors, namely, fundraiser-related, project-related and platform-related factors, to examine the trustworthiness of a crowdfunding project. The

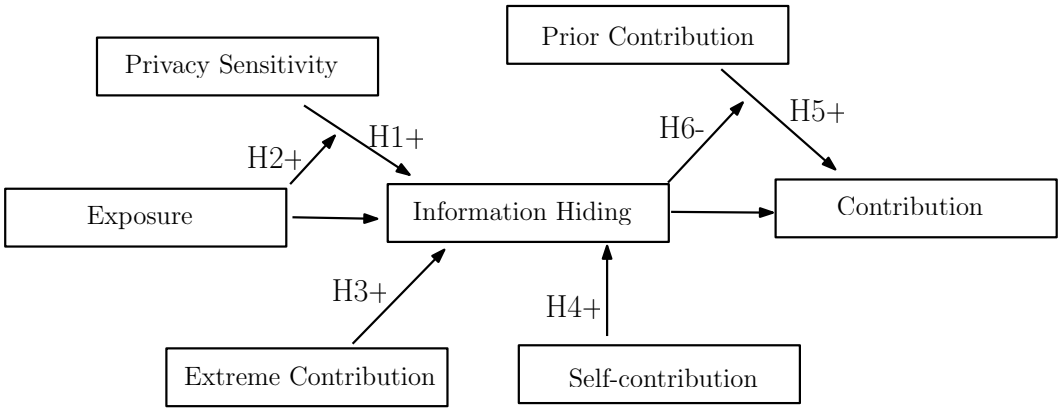

Fig. 4. The econometric model proposed by Burtch *et al.* [24, 25]. The likelihood of information hiding and the amount of contribution from crowdfunders are affected by the six hypotheses shown in arrows. The six hypotheses are privacy concern effect (H1), exposure effect (H2), extremity effect (H3), self-contribution effect (H4), anchor effect (H5) and censorship effect (H6). The positive or negative effect is denoted by +/- sign.

fundraiser's credentials were analyzed by a bootstrapping method that is based on historical investment experiences. However, their conclusion was based on a small size survey dataset from only one country, which was not validated via cross-sectional survey methods.

All reviewed works for privacy issues in crowdfunding practices are listed in Table 2. Each reviewed work is accompanied by its reference, year, main objective, proposed solution and major insufficiencies. Certain levels of privacy protection, as well as sacrifices, are hidden key factors for successful crowdfunding practices. With a well-established privacy protection protocol, crowdfunders are more willing to contribute because of a safer environment. However, in some situations, a certain degree of acceptable and controllable privacy sacrifice can be helpful for a successful crowdfunding practice. The fundraisers and platforms have to realize that the net funding is directly proportional to their reputations. One future trend is to develop a more sophisticated platform for protecting the funder information. For example, a hierarchical encryption system can be built to serve the basic crowdfunding purposes and allow the fundraisers to select different levels of information sharing with the public for various purposes. Moreover, as crowdfunding is a relatively new concept to people in the cyber-enabled world and is directly related to assets, privacy issues are emerging and are considered important research topics in the development process of the cyber-enabled world.

2.3 Crowdtesting

Crowdtesting employs modern crowdsourcing technology to find a large group of testers to test software or products at relatively low costs [154]. The requesters post their requested tasks on the web; the testers select the tests on their own time, write down the test results and claim the payoff. It is reported to be more reliable, more cost-effective, and faster than traditional testing methods [117, 143]. An example of crowdtesting is PyBossa [114], which offers an open-source platform for customized crowdsourcing tasks that require human cognition, knowledge or intelligence. The objectives of a crowdtesting include the testing of usability, acceptability, task performance and the quality of the results.

In the process of crowdtesting, both requesters and workers post crowdsourced data on an online platform, e.g., testing tasks and results. Part of the crowdsourced data can be privacy related, e.g., the data can include the requester's unclosed data and tester's personal information. Therefore, the top priority for privacy preservation

Table 2. References, main objectives, proposed solutions and important insufficiency of the surveyed works for crowdfunding.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Burtch *et al.* [24, 25]	2013, 2014	Studying the relationship between security and willingness	An econometric model	Not taking the full consideration for factors that may influence the crowdfunders' decisions
Burtch *et al.* [26]	2015	Showing the hidden cost of protecting crowdfunders' privacy utilizing modern techniques	Online randomized experiments	Experiment users are given complete freedom for their fund contributions
Zheng *et al.* [156]	2016	Analyzing the importance of trust management	A research model based on the elaboration likelihood model	Focusing on the trust management and ignoring other highly influential factors
Kang *et al.* [70]	2016	Revealing the fundraiser's true motivation for crowdfunding	A structural equation modeling technique	The survey dataset is small in size and limited to only one country

in crowdtesting is to protect user privacy in the data collection process. Harkous *et al.* [56] noted that users usually had difficulties in accessing the privacy levels of their shared data. They proposed a context-aware framework that is based on item response theory (IRT) for identifying the privacy risk of shared data on a cloud server. Comprehensive experiments on synthetic data were performed to show the effectiveness of their method, where data privacy levels were automatically assigned without user interaction. The main limitation of their work was that they did not address and discuss the ways of protecting user privacy immediately after identifying the risky data items. No policy or computing technique was proposed in their work.

Existing data protection schemes focus on encryption/masking algorithms. Kandappu *et al.* [69] showed how easily privacy leakage can occur with online survey platforms, such as MTurk and Google Consumer Surveys [95], which are also frequently used for crowdtesting practices. A customized survey platform called Loki was developed to allow users to choose their preferred security level before proceeding to the online survey. The actual survey results were masked by noises before being sent out for evaluation. Their work has two main limitations. First, the accuracy of the survey result was decreased due to the added noise. Second, there was no guidance for the user in choosing the appropriate security level; and the selection of security level eventually affected the overall accuracy of the final survey results.

Li *et al.* [81] identified the privacy issues in indoor site survey practices using the WiFi fingerprint-based localization technique. An indoor site survey task that is proposed by the service provider requires multiple suppliers to visit various places and send back WiFi signals. The entire process is usually performed in a crowdsourced manner, which is similar to crowdtesting practices. In [81], Li *et al.* intended to hide the location information of the suppliers from the service provider and simultaneously ensured the usability of the sent signals. However, a homomorphic encryption scheme was used, which means the original measurement signal was twisted before being sent out.

Although the crowdtesting service provides an innovative way for service providers to test their products with a large population of testers and relatively low costs, the privacy issues were never well addressed to protect

the sensitive information of the testers. Three specific applications of the crowdtesting practices are surveyed in this subsection: shared data protection on the cloud servers [56], online surveys [69] and indoor site survey practice [81]. The objectives, solutions and main insufficiencies are listed in Table 3. Almost all reviewed works demonstrate that user privacy can be easily breached by the service providers and platforms during the process of crowdtesting. Various techniques were proposed to identify risky shared data and protect those sensitive data pieces. However, encryption or masking of the original data affects the usability of the final testing results, which limits the use of these techniques.

Table 3. References, main objectives, proposed solutions and important insufficiency of the surveyed works for crowdtesting.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Harkous *et al.* [56]	2014	Identifying risking data pieces on cloud server	A context-aware framework based on item response theory (IRT)	Not discussing the way to protect privacy
Kandappu *et al.* [69]	2013	Allowing users to choose security level for online surveys	A customized survey platform called Loki	No guidance for the user to choose appropriate security level
Li *et al.* [81]	2016	Hiding the location information of the suppliers in indoor site survey practices	A homomorphic encryption scheme	The original measurement signal was twisted

2.4 Summary and Discussion

In conclusion, in crowdsourcing practices, there are always three roles in the model: the user, requester and platform. On one hand, the requester has the responsibility to protect workers' data privacy. He or she may not disclose or misuse user data without the consent of the workers. On the other hand, the requester designs mechanisms or protocols that discourage workers from leaking sensitive data of the tasks; and the workers are responsible for following the privacy agreements of tasks. The platform serves as a mediator that protects the privacy of both parties. Both the task requester and the users must understand that there are always tradeoffs between privacy and interests (e.g., incentives, task quality, funds). Both entities must sacrifice part of their privacy to enjoy a quality crowdsourcing practice.

While most of the works that are surveyed in this section focus on cyber technology development on the platform for protecting the privacy of both the task requesters and workers, some policy/regulation works are mentioned as supplementary materials. Although the business models of these three crowdsourcing practice branches are different, raising the privacy protection level is always helpful to both the workers and task requesters in achieving their goals.

In general, on a crowdsourcing platform, users should be allowed to retrieve information from the database of a sharing service provider while the queries are maintained privately. In addition, to increase the security level of data protection for users, data de-identification methods are available in most cases [44, 51, 53, 134]. Traditional methods, such as $k-$anonymity, $l-$diversity models and etc., can also be used to avoid linkage attacks [11, 119, 120].

3 PRIVACY ISSUES AND SOLUTIONS IN COLLABORATIVE CONSUMPTION PRACTICES

Unlike crowdsourcing, which combines the power of individuals to perform tasks, collaborative consumption allows an individual to access goods or services through P2P sharing, which is coordinated by online services [13, 21]. In collaborative consumption practices, hosts provide shared goods or services through a platform to the customers. The sharing methods include selling, borrowing, trading and sharing; typical examples of collaborative consumption platforms include eBay, Craigslist, Uber (ridesharing) and Airbnb (homesharing) (Figure 5). Collaborative consumption has many benefits, such as reducing greenhouse gas emissions, saving costs, providing access to unaffordable goods, and increasing independence and flexibility by decentralization [21, 54]. Although collaborative consumption has many advantages, it suffers from privacy concerns that limit its development. In this section, we review problems and solutions of privacy protection in collaborative consumption.

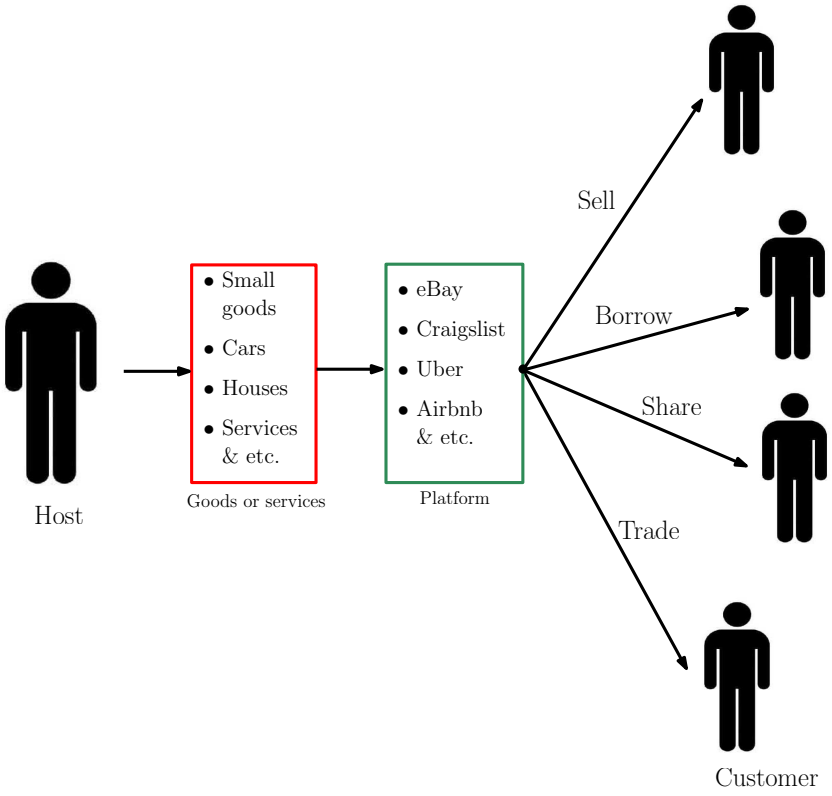

Fig. 5. A typical demonstration of collaborative consumption: hosts provide shared goods or services through a platform to the customers. The sharing methods include selling, borrowing, trading and sharing; the typical examples of collaborative consumption platform include eBay, Craigslist as well as Uber (ridesharing) and Airbnb (homesharing).

3.1 Collaborative Online Shopping

Online shopping is probably the first successful model in which cyber technology has changed our living world. In the first stage of online shopping development, people found that it was more convenient and economical to purchase goods over Internet. In the process of cyber technology development, the concept of collaborative

consumption was gradually embedded into the online shopping experience. People started to sell small items, trade services, share cars and borrow items through online shopping websites [21].

On the other hand, online shopping websites have received many criticisms due to their notorious privacy policies despite their popularity [22, 83, 129, 135, 151]. Although it is illegal to reveal user information to third parties without user consent, online platforms are not subject to a penalty for analyzing user data. These platforms may rely on third-party organizations for data analysis, which might deteriorate customers' privacy. The privacy policy terms are supposed to be accepted by customers without negotiations, which is in some sense unfair to the customers. Except for limited government regulations, these marketplaces are self-regulated or autonomous, which makes it difficult to protect consumer's privacy. Moreover, these platforms suffer from data leakage due to cyber attacks or intrusion. These factors contribute to the vulnerability of consumers' privacy.

Miyazaki and Fernandez [99] surveyed about online shopping fears on a set of U.S. Internet users from different age groups, economical classes and educational backgrounds. The survey results indicated that the untrusted security system is the largest fear of the customers. Malhotra *et al.* [94] systematically analyzed Internet users' information privacy concerns (IUIPCs) through two separate surveys of 742 household respondents. They designed a theoretical framework for studying IUIPCs and proposed a causal model that predicts the reaction of online customers to privacy threats from shopping websites. Tsai *et al.* [133] studied how the privacy concerns of customers affected their decisions in the online shopping process. They conducted an experiment to test the shopping decisions that were made by customers after displaying their personal information on the shopping websites. Their results demonstrate the customers' willingness to pay a premium for extra privacy protection (from a more expensive shopping website). All of the above mentioned works reveal the fact that the privacy concern is the main fear in online shopping experiences. However, these works do not present a deep analysis for how to build privacy protection trust between online shopping websites and customers.

Shiau and Luo [126] built a research model using partial least squares (PLS) analysis to indicate the relationship between the consumer satisfaction, the intention of online group buying and user beliefs (Figure 6). The PLS analysis results show that consumer satisfaction highly depends on trust, followed by reciprocity. It is the first work to draw an overall picture of the different factors that affect the online shopping decisions. Moreover, it is also the first work to clearly identify privacy concern as the first priority for online shopping security. Following Shiau and Luo's work, Bergström [18] built an analytic system with different groups of people concerning various privacy issues in online shopping experiences. Both the customers and the privacy concerns were partitioned into different dimensions to interpret the links between socialization, Internet experience, trust, politics, and security understanding. Their analysis result clearly indicated that the trust is the major concern of people who worry about the misuse of personal data. Although these research models go one step further than the simple survey results, they still do not provide a clear solution for protecting the online customers' privacy.

Preibusch *et al.* [113] studied and reported a concrete example of privacy leakage in online shopping practices. They performed online tracking and found that online shopping websites send unnecessary personal information to payment providers, such as Paypal. Therefore, there is an on-going risk for customers who shop online. The most effective method for changing this situation is to facilitate relevant legislation. However, the lack of government regulation of online shopping websites exists globally. Moreover, it remains unclear what rules might be added and how they can be enforced. Although there are existing regulations (Directive 95/46/EC by the European Union [112] and USA Patriot Act [72]), studies have shown that those regulations are usually ignored due to insufficient legal actions.

Another possible solution from the user end is to install third-party privacy protection software in the web browser. Available software on Internet includes the Tor Browser [91], the Privacy Bird [142] and the Platform for Privacy Preferences [111]. These third-party software programs or plugins identify untrusted shopping websites and mask personal information for the customers. However, third-party software is usually not formally authorized or registered by the government, which potentially raises other concerns of privacy leakage.

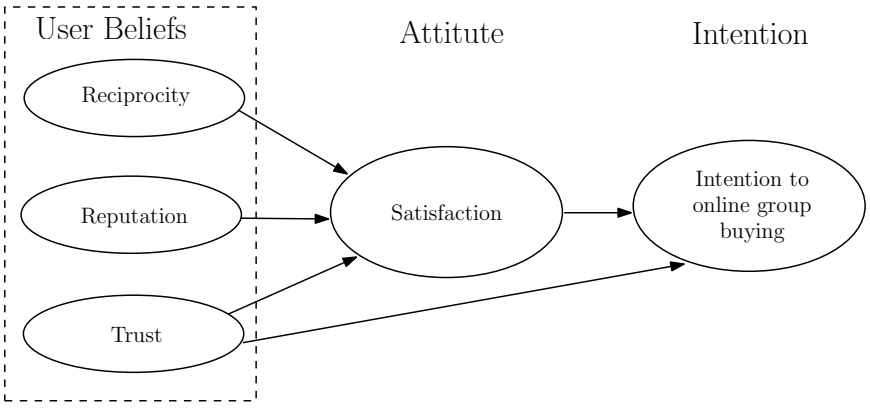

Fig. 6. The research model proposed by Shiau and Luo [126], showing the relationship between consumer satisfaction, intension of online group buying and user beliefs.

Lee *et al.* [79] proposed a π-box mobile app for controlling the sensitive data transmission between different users and from users to service providers. The π-box extends the user apps and was built based on the cloud services that were supplied by large companies, such as Google. Two separate channels were designed: the sharing channel, which controls the data transmission between users and the aggregate channel, which controls the data transmission from users to the service provider. The structure of π-box is illustrated in Figure 7. All channels are internally monitored by π-box; therefore, the privacy preservation is guaranteed. Nevertheless, according to the user evaluation, not all apps support π-box. Only 48% of paid apps support π-box, which limits its use.

Kokolakis [76] studied the conflict between the customer's high demand for privacy protection and the customer's willingness to sacrifice privacy for the exchange of goods or services in the online shopping practice. Kokolakis concluded that this inconsistency represents a collision between a customer's attitude and behaviour, which is known as the privacy paradox [106]. A large volume of works was surveyed to justify the existence of the privacy paradox; however, most of them are survey or experimental works that do not consist of theoretical model.

Bilge and Polat [20] introduced a method for improving the online shopping experience by collecting customers' personal information, such as ratings of specific services or products, in a privacy-preserving manner. A number of clustering methods were integrated into the collaborative filtering service, where the system learned the masked customer data using clustering methods and filtered out unwanted/inappropriate information for the customers. However, due to the masking of personal data, the recommendation error rates increased. In addition, the clustering methods introduced extra computational costs into the recommendation system.

The reviewed works, which are listed in Table 4, identified two privacy threats in collaborative online shopping practice. The first threat comes from the service provider, where unreliable platforms may misuse customers' data for marketing analysis. This threat can be prevented by refining government regulations [113], masking customers' data before sending them out [20] or separating communication channels on the cloud server [79]. The second threat comes from the customer side, where most customers realize that they must sacrifice a certain degree of privacy to enjoy the collaborative shopping experience [76]. It is difficult for them to choose a trustworthy service provider, products [18], and most importantly, the kinds of permissions to grant [64]. The second threat can be alleviated by increasing the overall privacy awareness of the users, which will be extensively discussed in Section 4.1.

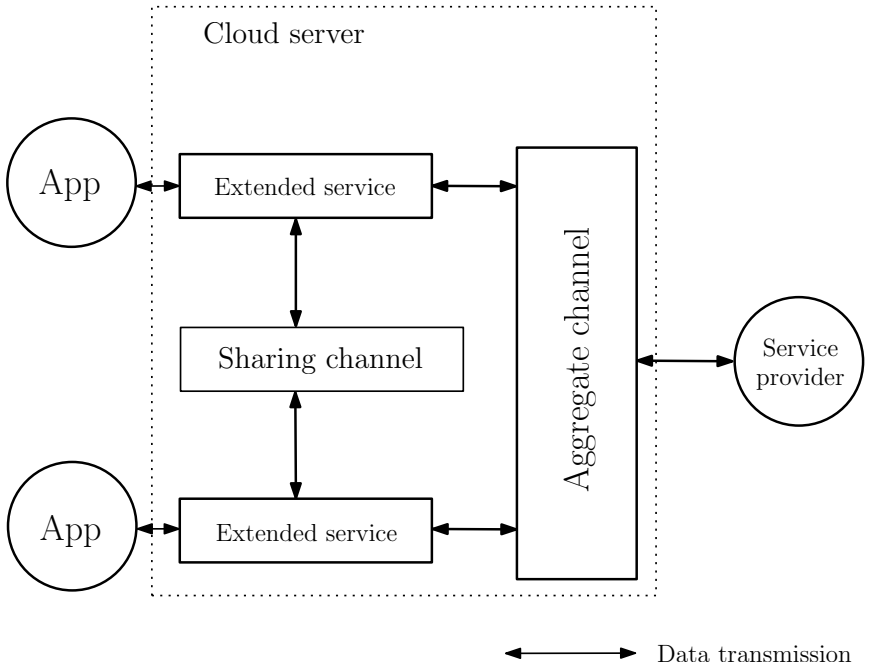

Fig. 7. The internal structure of π-box: it extends the user apps on cloud server. Two separated channels were designed, which were the sharing channel controlling the data transmission between users and the aggregate channel controlling the data transmission from users to the service provider.

3.2 Ridesharing

Real-time ridesharing or dynamic carpooling is a transportation service that allows commuters to share rides on very short notice through mobile apps [1, 30, 123–125]. Successful ridesharing platforms, such as Uber, are available in most major cities in the world. When a user needs a ride, he/she may simply use a mobile app to request a ride by entering the destination. The app provides the estimated cost and assigns a driver to the passenger. The payment is generally made with the credit card or other digital payment methods that are associated with his/her account. In the end, both the passenger and the driver will rate each other.

Obviously, the mobile app tracks the customers' location information and travel information. The driver also has access to the rider's travel information, such as riders' names, trip starting points and destinations. Under current privacy policies, riders have to share some of their private information to receive services. The platforms have limited regulatory power over the drivers because the drivers are contractors rather than employees of the ridesharing companies. Moreover, drivers' names and license plate information are also subject to disclosure. Concerns have been raised about the internal misuse of user data within the ridesharing companies. For instance, staffs in the ridesharing companies have the access to data for tracking the movements of customers. Taking Uber as an example, in its user agreement terms, it is clearly stated that user information, such as the geo-location, is recorded and internally used by the company for research development purposes. However, the purposes of internal research are not defined explicitly. Customers may worry about how their private data is used. Additionally, Uber can access, use, preserve, transfer and disclose user information to prevent, discover or investigate violations of the privacy policy or the user agreements as determined necessary or appropriate' [73] by Uber. However, customers do not know what information is necessary or appropriate.

Table 4. References, main objectives, proposed solutions and important insufficiency of the surveyed works for collaborative Online Shopping.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Miyazaki and Fernandez [99], Malhotra *et al.* [94], Tsai *et al.* [133]	2001, 2004, 2011	Pointing out the biggest fear for online shopping experiences	Surveys on Internet users	Lacking a deep analysis to build the privacy protection trust between the online shopping websites and the customers
Shiau and Luo [126], Bergström [18]	2012, 2015	Learning the largest privacy concern in online shopping practices	Drawing the overall online shopping fears relationships by research models	No clear solution for protecting the online customers' privacy
Preibusch *et al.* [113]	2016	Pointing out the need of raising government regularization for online shopping globally	A concrete example of the privacy leakage in online shopping practices	What rules to be added and how to add are two big questions
Lee *et al.* [79]	2013	Separating the data transmission from user to user and from user to service provider	A mobile app called π-box	Not supporting all paid apps
Kokolakis [76]	2017	Revisiting the conflict known as 'privacy paradox'	A survey covering related existing works	No theoretical model was discussed
Bilge and Polat [20]	2013	Protecting privacy in user information collection process for a recommend system	Masking sensitive data and using clustering methods for data analysis	Losing analysis accuracy

Location privacy has been studied extensively in recent decades because of the pervasiveness of geo-location related software and mobile apps [10, 17, 19, 98, 122]. While location-aware applications track customers' location or other data online, they generate a huge amount of potentially sensitive data. The privacy of location data depends on the regulation of data access. It is neither necessary nor possible to forbid all accesses because the systems must access the data for analysis purposes. Moreover, access permissions should be given to authorized persons and should never be exposed to others. In other words, the data and the access should be tightly controlled and data should be accessed only with legal authorization [17].

Kido *et al.* [74] proposed one of the first techniques for concealing the actual locations of customers in location-based services, including ridesharing practices. When a user sends an inquiry to the server, he/she sends his/her actual location, together with two false positions called 'dummies.' The dummy nodes in the tracking system are carefully generated such that an observer cannot easily identify the actual location of the user; however, the location-based server (LBS) can find the difference through optimized algorithms with external information such as road navigation service (RNS) data. The obvious shortcoming of Kido *et al.*'s work is that the real location is not completely concealed. There is still a chance that the observer will identify the actual location.

Yao *et al.* [152] provided an effective encryption service for location information of customers with the clustering K-anonymity (CK) scheme [119]. The CK scheme encrypts the user location information by utilizing a cloaked spatial-temporal boundary (CSTB) that involves K users. The spatial and temporal constraints, which determine the resolution of the encryption, can be personalized by users. However, the use of CSTB decreases location information resolution, and consequently, degrades the quality of service (QoS).

Pan and Meng [109] extended Yao *et al.*'s work using a *p*-anti-conspiration model for location privacy protection of customers. Various techniques were introduced, including methods for providing LBS without knowing the actual locations of the customers. It is a large advancement for the ridesharing companies in protecting the user locations. A follow-up work by the same group of authors in [108] showed that the shortcomings still exist in the aspect of protecting sensitive information.

Jagwani and Kaushik [65] introduced the concept and structure of the zero knowledge proof (ZKP) to defend against location information leakage. They explained the detailed construction process of ZKP and discussed the possible applications of ZKP in the location-based service domain. The main shortcoming of the ZKP approach is that a platform is always required to coordinate between customers and hosts.

Gao *et al.* [50] noted that trajectory privacy, which contains spatial-temporal information, must be added to location privacy protection schemes. In their study, they proposed a trajectory privacy-preserving framework for protecting trajectory privacy. A mixed-zone graph model is employed to illustrate the proposed framework. However, again, the exact location is revealed to a third party middleware.

In recent years, online social networks or geosocial information have started to be used in ridesharing services. It is obviously preferable to use a friend's car rather than stranger's. Based on this motivation, Elbery *et al.* [45] proposed a social Vehicular Ad-Hoc Network (S-VANET) carpooling recommendation system. They embedded friendship locality, preference locality, and travel locality information into the ridesharing recommendation system, which requires a large amount of privacy information from both the requester and his/her friends.

Ni *et al.* [104] suggested that customers' true identities can be hidden by incorporating an anonymous mutual authentication (AMA) protocol into the carpooling recommendation system. A real-time navigation system is proposed for concealing the drivers' privacy [103]. One important feature of their application system is the false information traceability, where the trusted third party authority can trace incorrect information, either from a user or a driver. The main limitation of their work is that a trusted third party is still required.

Aïvodji *et al.* [3] proposed a privacy-preserving local computational method for determining the meeting point of a driver and a rider in a ridesharing system, which does not require third-party middleware. Multimodal routing algorithms are used to compute a mutually interested meeting point for both the driver and rider. More complicated systems that involve multiple drivers and riders are left for future exploration.

Shokri *et al.* [127] concluded that the current location privacy research mainly focused on three aspects: perturbing the actual location, tracing the perturbed location, and evaluating the privacy-preserving methods. While most existing works only focus on encrypting the customer's current location, strategies might be employed by attackers to trace down the actual location of the customer. Useful private information pieces, such as recently visited locations, frequently visited places and nearby landmark buildings, become potential clues for the attackers in estimating the current location of the customer. In [127], a comprehensive Bayesian security game is designed to simulate various cases in which a strategic attacker traces the actual location of a customer. Four different scenarios were studied. However, it was difficult to predict the intelligence level of the attacker; and the whole simulation system is too complex in most real-world scenarios.

Vergara-Laurens *et al.* [140] categorized privacy preserving systems into approaches for two processes: the tasking process, where tasking devices (such as mobile phones) collect data in certain areas, and the reporting process, where distributed devices report sensed data to the platform. Both processes exist in ridesharing practices. Vergara-Laurens *et al.* summarized almost all location privacy preserving techniques in their taxonomy.

Moreover, they provided three open problems for researchers in the field of location privacy preservation, which indicate the future working trends in that field.

Table 5. References, main objectives, proposed solutions and important insufficiency of the surveyed works for ridesharing.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Kido *et al.* [74]	2005	Protecting location privacy using dummies	An anonymous communication technique	The actual location is not completely concealed
Yao *et al.* [152]	2010	Encrypting the user location information	Clustering K-anonymity (CK) scheme	Decreasing location information resolution and degrading the QoS
Pan and Meng [109]	2013	Providing location-based services without knowing the exact location	The p-anti-conspiration privacy model	lacking protecting sensitive information
Jagwani and Kaushik [65]	2012	Removing the dependency of using third party software	Zero knowledge proof	A third party middleware is required
Gao *et al.* [50]	2013	Protecting the trajectory privacy	A trajectory privacy-preserving framework	The exact location must be revealed to a third party middleware
Ni *et al.* [103, 104]	2016	Concealing both customers and drivers' sensitive information	An anonymous mutual authentication (AMA) protocol	A trusted third party is required
Aïvodji *et al.* [3]	2016	Computing the mutually interested meeting point	Multimodal routing algorithms	A more complicated system involving multiple drivers and riders are left for future exploration
Shokri *et al.* [127]	2016	Considering strategic attackers for customer's location privacy	A comprehensive Bayesian security game	The complexity may not be necessary for most of the real-world scenarios
Vergara-Laurens *et al.* [140]	2017	Surveying privacy-preserving mechanisms	A survey of all existing works on location privacy preservation	Only location privacy is heavily surveyed

All reviewed papers are summarized in Table 5. Similar to other sharing services, customers may realize that a certain degree of their privacy must be sacrificed to enjoy better service quality. Taking the Uber service as an example, the platform (Uber app) usually records the customers' private information, including current location, destination, phone number, recent trips and so on, to serve them better. However, the customers sacrifice their privacy to enjoy the Uber service. The tradeoff between the disclosure of private information and the service quality becomes more obvious in the ridesharing practices, which is also mentioned in most of the surveyed works, such as [3, 50, 103, 127].

Compared to other fields of sharing service, ridesharing is a relatively new technology. Few regulations have been established in this area; and most privacy concern solutions are on technical aspect. Despises the variety of technologies proposed by the existing works, only location privacy is extensively discussed. Ridesharing

services include direct interpersonal interactions (IPIs), e.g., the conversation between the rider and the driver when they are travelling [7, 36, 141]. Computerized technologies, which are designed to be embedded in the online platform, can be helpless in IPI; and physical privacy concerns exist at this stage [37]. Physical privacy concerns, which were first defined by Belk, occur when the driver or passage's personal space is invaded, where we refer to the remaining privacy concerns as online privacy concerns [12, 14]. For future works in this field, we would like to note that physical privacy protections for both the riders and drivers are demanded in the ridesharing practice.

3.3 Homesharing

Homesharing is a business model that connects hosts and travelers through an online marketplace platform and enables transactions without the platform owning any rooms itself. It does not provide the rental services directly. Instead, it matches hosts who have extra rooms for rent and travelers who need a room for stay [49, 110]. One of the most famous homesharing platforms is Airbnb [66].

The face-to-face e-commerce model makes the physical privacy issue more serious for homesharing practices compared with online sharing model. The host and traveler usually meet each other before a deal was made and both of them have the possibility to reveal the privacy of each other to the public. For example, a host might install a hidden camera in an Airbnb room to monitor travelers. A traveler might take pictures to reveal the details of the room or other parts of the house to the public. The online platform records sensitive information of both the hosts (e.g., names, travel plans) and the travelers (e.g., names, home locations).

Kamal [68] noted that the largest inhibitor of homesharing services is the fear of privacy disclosure. Additional background checks are necessary for participants in homesharing activities, with the possibility of more security measures, such as certificates and safety insurance. The cost comparison between homesharing with additional security checks and hotel accommodation is not discussed.

Morosan and DeFranco [102] determined the level of willingness of travelers to disclose their personal information to hotel apps. An extended version of the privacy calculus model was adopted. The experimental results indicated that personal information disclosure was indeed helpful for the hotel business, i.e., to choose the best customers. But the willingness to disclose such information was related to privacy concerns, trust, emotions and etc. However, the study was conducted based on data that were collected from U.S. customers who were involved in a relatively safe environment with reliable network security, regulations, and hotels. The results may not be applicable to developing countries.

Ert *et al.* [46] designed an experiment that used mixed-logit analysis to determine the relationship between the posting of a host's photo in the advertisement and the booking likelihood. The results show that both the trustworthiness and attractiveness of the host's photo increase the likelihood of the house being booked. Nevertheless, the positive correlation between trustfulness and privacy protection was left for further exploration in their work.

The risks of being a host, including the posting of the host's photo and identity information, in the homesharing practices are discussed by Hooshmand [61]. The leakage of the hosts' privacy is another issue in homesharing practices.

Lutz *et al.* [87] explicitly divided the privacy concerns into physical privacy concerns (e.g., physical damages of private assets) and online privacy concerns (e.g., personal identity leakage). They conducted a survey on MTurk involving 389 participants; and most of them were hosts on Airbnb. The survey results showed that physical privacy concerns are more crucial than online privacy concerns in the homesharing business. The main shortcoming of their work is that the survey is limited to Airbnb hosts and does not include any customers. Thus, the survey results may be biased towards the hosts' preferences.

We list all reviewed works for security concerns of homesharing in Table 6. Compared to other sharing services, homesharing involves more interpersonal interactions; therefore, concerns about physical privacy are

heavily studied in this field. Most of our surveyed works agreed that the hosts are more concerned about their privacy leakage than the travelers. Future studies can focus more on the development of privacy protection schemes for hosts. In the current stage of homesharing, while it is unlikely to solve the privacy issue with a single method, it is quite possible to provide a general privacy-preserving environment for both hosts and travelers through the joint efforts of hosts, travelers, platforms, and governments.

Table 6. References, main objectives, proposed solutions and important insufficiency of the surveyed works for homesharing.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Kamal [68]	2016	Building trust in homesharing practices	Proposing additional security checks	Not discussing the cost of additional security measurements
Morosan and DeFranco [102]	2015	Checking the willingness of hotel customers to disclose personal information	An extended version of the privacy calculus model	Collecting data only based on U.S. customers
Ert *et al.* [46]	2015	Showing the relationship of posting a host's photo and the booking likelihood	Mixed-logit analysis	The relationship between trust and privacy might be of interest but not discussed
Lutz *et al.* [87]	2017	Investigating the impact of physical privacy concerns to homesharing	A survey on MTurk	Only hosts were surveyed

3.4 Summary and Discussion

Collaborative consumption collects extra or redundant information resources and distributes them to people who do not have access to them. For example, in the collaborative online shopping scenario, customers are subject to privacy leakage due to the exchange of data and improper use of user data by internal staffs of the platforms. Similar to crowdsourcing practice, both hosts and customers must understand that certain degrees of their privacy have to be sacrificed for better service quality. While it is difficult to provide an absolute privacy-safe environment without sacrificing service quality, it is possible to increase the protection levels of privacy through a joint effort of all participants, platforms and governments.

Compared with collaborative online shopping, both ridesharing and homesharing involve more interpersonal interactions (IPIs). For ridesharing, location privacy is separated from the general concept of privacy and is extensively studied and discussed. For homesharing, the general form of privacy is further divided into online privacy (electronic forms of personal information) and physical privacy (human body, house, furniture, etc.) [87]. There are works showing that the physical privacy concerns are more important than online privacy concerns for homesharing. We believe that the concept of physical privacy will be considered in privacy protection studies in other areas in near future, such as ridesharing.

Other methods are available for protecting privacies in collaborative consumption practices. Milberg *et al.* [97] studied various aspects that affected the customers' willingness to participate in collaborative consumption in the early 1990s. The study shows some early efforts and results from governments in designing suitable regulations for protecting the customers' privacy. Luo *et al.* [86] examined several mechanisms to demonstrate the close

relationship between trust and privacy preservation. Nissenbaum [105] discussed privacy from the perspective of contextual integrity in technology, policy, and social life.

4 SUMMARIZING EMERGING PRIVACY ISSUES FROM THE USER, PLATFORM AND SERVICE PROVIDER PERSPECTIVES

Fast development of cyber technology facilitates the invention of novel sharing practices in the cyber-enabled world. While traditional privacy problems have either been solved or at least realized by the government and society, privacy issues in cyber-enabled sharing services are less well understood and emerging. In all six branches of the taxonomy in Figure 1, there are always interactions between users, platforms, and service providers. The privacy protection issues were always discussed from these three perspectives in the reviewed works.

In this section, we discuss that all privacy issues from different applications are internally related. Users concern with their own privacy and always demand high quality reliable sharing services. Service providers must realize that privacy protection is a key element towards a successful achievement. Anybody involved in the sharing service can be a potential attacker to compromise other people's privacy. The linkages between the privacy concerns from the three perspectives are shown in Figure 8. We show that the emerging issues for sharing services are: increasing users' privacy awareness from their perspective, protecting shared information from the platforms' perspective and making privacy concerns the top priority from the service providers' perspective. Works that are surveyed in this section are listed in Figure 9 and summarized from the three perspectives.

4.1 From Users' Perspective: Increasing Privacy Awareness

Although most websites, software and mobile apps provide user agreements for user privacy awareness, only a negligible portion of users read through the tedious clauses carefully. The first emerging privacy issue for cyber-enabled sharing services is to maximize user awareness of privacy leakage, e.g., to provide an online tool for users to trace down entities that may reveal their personal information. The transparent information tracing system will increase the confidence of users in participating in sharing practices on Internet, as well as facilitating the service providers to improve their reputations.

For example, in the crowdsourcing marketplace, it is not sufficient to protect only requesters' data privacy because workers also value their privacy equally. Workers are commonly afraid of the leakage of their location data or the identity information (e.g., age, contact, hobbies, activities) [132, 150]. According to a survey that was performed by the U.S. Federal Trade Commission [38], more than 85% of users were too impatient to read the user agreements regarding privacy settings carefully. They were surprised that mobile phone apps sent their approximate or precise location, phone's unique ID to service providers. Some apps even have control of the camera flashlight and audio settings. Although these privileges were authorized by users, they did not know when or where they give the authorizations, because they never read the articles about the privacy settings. Some efforts have been made to solve the above problem.

Malandrino *et al.* [92, 93] implemented a privacy awareness software, which is named as 'NoTrace'. The software provides services, such as automatic settings for protecting privacy, measurement of the personal data that have been revealed to the the service provider and awareness of privacy leakage to third-party websites. The graphical user interface of 'NoTrace' is shown in Figure 10, which clearly displays the privacy elements that are received by the service provider. However, they did not provide a deep analysis of which data elements are necessary for the service and which are not. The analysis provides useful hints for users, as well as the service provider, regarding selective sharing of private information.

Omoronyia *et al.* [107] proposed an adaptive privacy framework for assisting privacy disclosure decisions that are made by applications. The framework is designed following the famous MAPE (Monitor, Analyse, Plan and Execute) loop, and is focused on three aspects: application attributes, potential privacy threats and derived

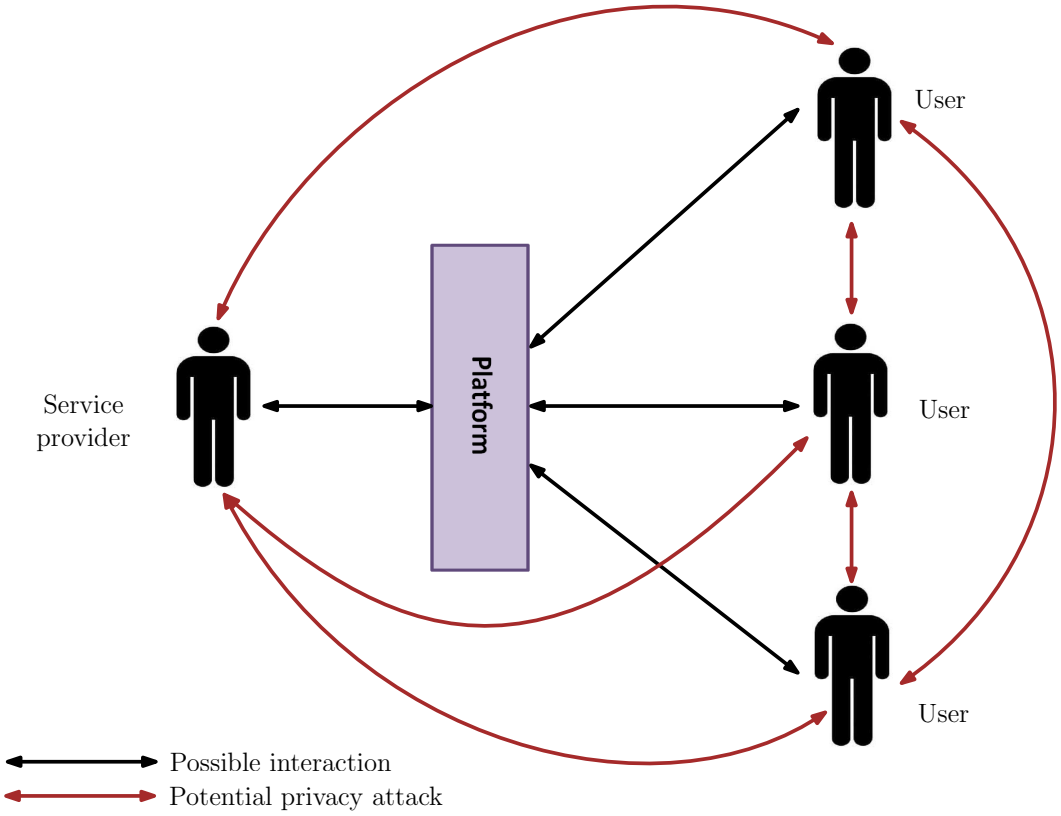

Fig. 8. The privacy relationships between the user, platform and service provider. For any participant in the sharing practice, no matter he/she is a user or service provider, all the remaining people involved in the same sharing practice can be potential attackers to compromise his/her privacy.

benefits from privacy disclosure. The main shortcoming of their work is that it lacks a list of systematical privacy requirements for a given set of service functions [96].

Amini *et al.* [4, 5] developed a software called AppScanner to help users better understand the functionalities of mobile applications. The software provides an informative descriptions of what mobile apps are really doing under a crowdsourcing environment. The transparency and detailed analysis of the mobile apps help make users aware of possible privacy leakage when using mobile apps for crowdsourcing. AppScanner only categorizes the mobile app behaviors as normal or abnormal. A detailed categorization according to the behaviors purposes, e.g., advertising and social networks, can be more helpful in user decision-making [148].

Zhu *et al.* [157] implemented a mobile app recommendation system with security and privacy awareness. The proposed system first analyzes the mobile application with detection and diagnosis of the security risks from insecure data access permissions. The software then provides a recommendation to the user on whether to continue using the mobile app according to the app's popularity and user settings. The recommendation is based on modern portfolio theory. The main shortcoming of the recommendation system is that the security risks are only evaluated based on the permissions that the apps request.

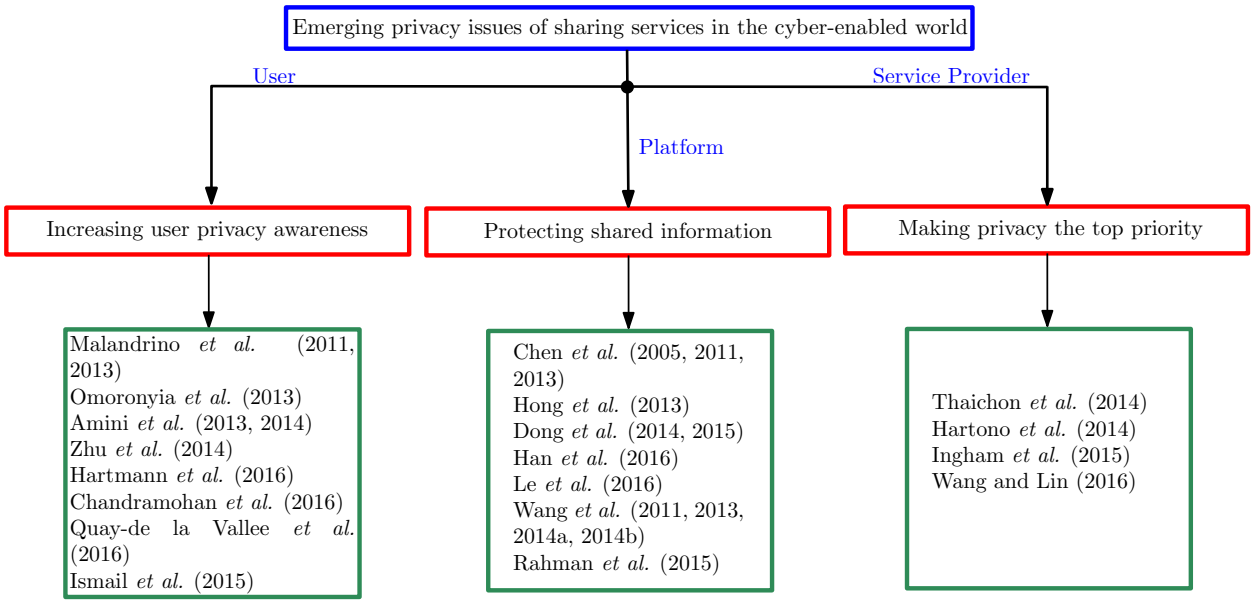

Fig. 9. The emerging privacy issues identified in the current stage of cyberized sharing service development from the user, platform and service provider perspectives. The emerging privacy issues are shown in the red boxes. All works surveyed in this section are listed in the green boxes.

Hartmann *et al.* [57] summarized six main threats of mobile apps to make the users aware of potential privacy risks: insufficient control features, excessive data mining, data theft, surveillance, information leakage and social engineering. They also proposed eight recommendations for guarding against these privacy threats: privacy dashboard, privacy policy, data handling guidelines, user permissions, anonymization, IT infrastructure security, encryption, and relationship. All the guidelines are valuable for future privacy-aware mobile application development. However, immediate solutions for all conflicts are still missing.

Chandramohan *et al.* [31] noted that over 90% of users accept user agreements unconsciously, without knowing that their personal information might be abused. They described a complete privacy-preserving scheme called Petri-net Privacy-Preserving framework that was installed on a cloud server. However, the practicability and real-time applicability of their algorithm need further discussion.

Similar to traditional websites that force users to accept user agreements, the mobile apps tend to mitigate the privacy risks to the users by requesting resource access permissions. Quay-de la Vallee *et al.* [115] developed two app systems that help users find privacy-respective apps and manage the apps' permissions in their mobile phones. However, the two systems only provide privacy management assistance after the apps have been installed, instead of providing the assistance during the installations process.

Ismail *et al.* [64] studied the possible privacy threats from mobile apps that require access to sensitive resources during the processes of installation or updating. A crowdsourcing strategy that identifies the minimal number of permissions to keep the mobile apps fully functioning for a diverse range of users was proposed. A user study that involved 26 participants and the popular mobile app 'Instagram' showed the effectiveness of their approach. However, the survey size was relatively small; and the method was only tested on a single mobile app. The usability of the proposed crowdsourcing strategy requires further justification.

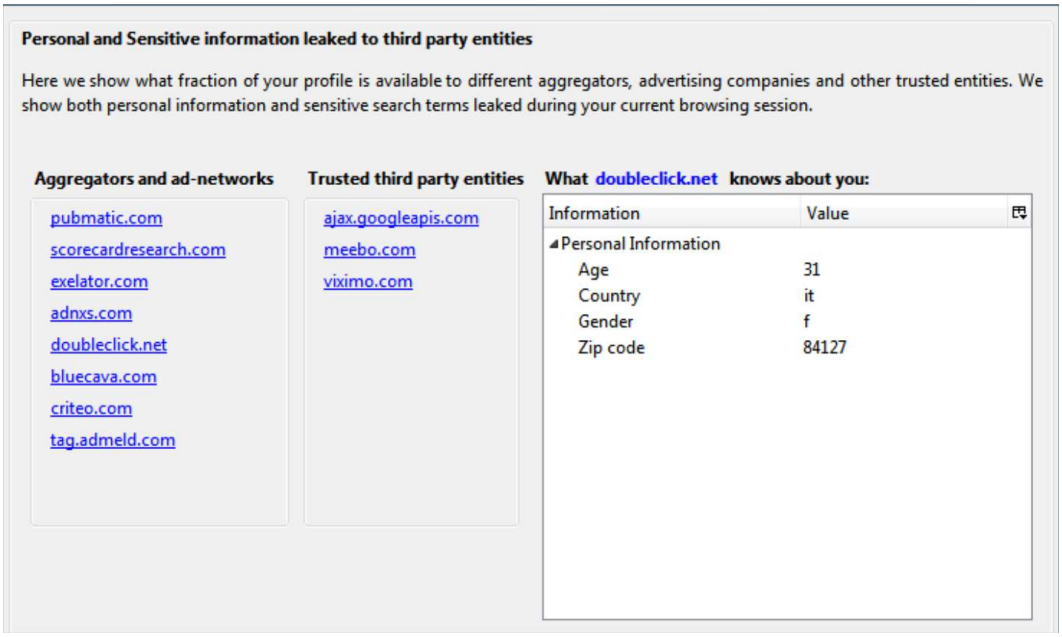

Fig. 10. The 'NoTrace' software graphic user interface, developed by Malandrino *et al.* [92, 93]. All personal information received by the service provider is listed in the white box.

In summary, all the above mentioned works, which we list in Table 7, suggest that privacy leakage on some level is unavoidable for users to enjoy the sharing service. However, user awareness of privacy leakage can be improved by listing possible threats from third-party websites/applications [4, 5, 57, 92, 93], recommending safe decisions to users [107, 157] and using cyber-technologies [31, 64, 115]. Although various techniques are proposed to raise the user awareness level, most sharing service platforms only provide user agreement terms to warn about possible privacy leakage. There is still a large gap between forcing users to agree to terms, granting access permissions to sensitive data and motivating users to actively protect their own privacy. Platform and service providers should be encouraged to use the existing cyber-technology to maximize user awareness of privacy issues. Future works and surveys can be conducted in this direction.

4.2 From the Platform Perspective: Protecting Shared Information

Although users may agree to share part of their personal information on the platform, the shared information/data is still required to be well protected from all potential attackers. Many third-party platforms use cyber technologies, such as cloud computing, to analyze shared user data. The purpose of data analysis is to achieve better service quality. However, privacy concerns make users reluctant to share sensitive information. The second emerging privacy issue is to establish an effective protocol for protecting privacy in the data analysis process. In this section, several existing works from the recent year from the literature for protocol design are surveyed.

Chen *et al.* [32, 34, 35] presented a random space encryption (RASP) scheme that produces secure privacy protection on the cloud. RASP provides service to transfer the analyzing data into an encrypted space with a two-stage encoding algorithm. In their study, they identified that updating the encrypted database is another challenge in their work.

Table 7. References, main objectives, proposed solutions and important insufficiency of the surveyed works for increasing privacy awareness.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Malandrino *et al.* [92, 93]	2011, 2013	Measuring revealed data by service provider and privacy leakage to third-party websites	'NoTrace' software	Lacking of analysis on necessary information disclosure for a known service
Omoronyia *et al.* [107]	2013	Assisting privacy disclosure decisions made by applications	An adaptive privacy framework	Lacking systematical privacy requirements listing for a given set of service functions
Amini *et al.* [4, 5]	2013, 2014	Helping users better understand the functionality of mobile applications	AppScanner	A detailed categorization according to the behaviors purposes can be more helpful
Zhu *et al.* [157]	2014	Recommending mobile apps to users with security and privacy awareness	A mobile app recommendation system	The security risks are only evaluated based on the permissions that the apps request
Hartmann *et al.* [57]	2016	Addressing threats of mobile apps and proposing solutions	Eight recommendations for six main threats	No immediate solution is provided
Chandramohan *et al.* [31]	2016	Protecting user privacy on cloud	Petri-net Privacy-Preserving Framework	The practicability and real-time applicability of their algorithm need further discussion
Quay-de la Vallee *et al.* [115]	2016	Managing apps's access permissions	Two management apps	The privacy management assistance was only provided after the apps been installed
Ismail *et al.* [64]	2015	Identifying the minimal number of permissions to keep the mobile apps fully functioning	A crowdsourcing strategy	The proposed strategy is only tested on one single mobile app

Hong *et al.* [60] surveyed several existing privacy protection strategies under the distributed data sharing environment. They noted that privacy protection techniques can be applied to the database, queries or aggregation. Specifically, they focused on privacy-preserving schemes for time series data processing for data mining.

Dong *et al.* [41, 42] suggested a security policy based on existing encryption techniques. The proposed framework allows the users to dynamically access their own personal data freely. Both attribute based encryption (ABE) and identity based encryption(IBE) were used to minimize the key management overhead; however, the proposed method resulted in key escrow problems [118].

Following Dong *et al.*'s work, Han *et al.* [55] provided a promising solution for privacy-preserved data outsourcing under the cloud environment. They proposed an attribute-based encryption (ABE) based control scheme on two major problems for data accessing privacy protection on the cloud. However, the time complexities of both the encryption and decryption processes in the proposed method were not optimized for the real-world use.

Le *et al.* [78] assumed that there were pre-defined rule regulations in the data processing scenarios. An inconsistency checking and removing algorithm was designed to ensure the enforceability for multi-access to stored data in cloud servers. The main concern of their approach was that the pre-defined regulations might not be applicable under certain conditions.

Wang *et al.* [85, 145–147] proposed another hierarchical encryption scheme. The general structure of the proposed scheme is illustrated in Figure 11. The trusted third party (TTP) maintains the access control for the domain masters. Each domain master generates keys to a specific group of users in the next sub-level. For example, the leftmost domain master acts similar to the office administrator who is in charge of all personnel in the office, but does not to administer any other attributes. In addition, they also proposed a scalable revocation scheme for users to access their own personal data. The proposed scheme lacked user revocation and was only applicable to the situation that all attributes were administered by the same domain authority.

Rahman *et al.* [116] reviewed 139 works from 2009 to 2014 regarding information security in cloud computing. Specifically, they focused on the incident handling strategy (IHS), which is an important tool for protecting data in a shared cloud service system. They pointed out that although IHS setup is straightforward on a personal computer, it becomes complicated when cloud computing allows multiple computers to access the same data on the same hard-disk. They proposed an information protection model for shared data on the cloud that combines IHS and digital forensics principles.

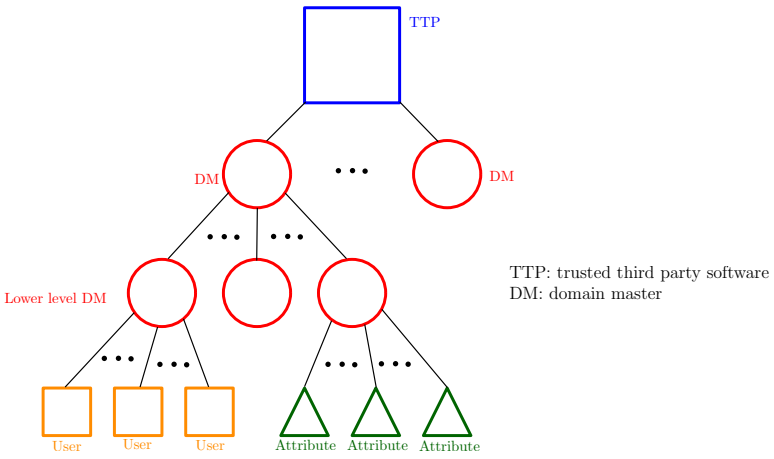

Fig. 11. The hierarchical encryption scheme proposed by Wang *et al.* [85, 145–147]: the trusted third party has the access control for the domain masters. The domain master generates keys to a specific group of users in the next sub-level. For example, the leftmost domain master acts like the office administrate who is in charge of all personnel in the office, but not to administer any other attributes.

In summary, a list of the surveyed works can be found in Table 8. From the platform point of view, there are mainly two parts of the data sharing practice can be worked on to provide more secure sharing services: the data transmission process and the data storage on the cloud server. To protect sensitive data during the data transmission process, data encryption is usually utilized [41, 42]. For data protection on the cloud server,

Table 8. References, main objectives, proposed solutions and important insufficiency of the surveyed works for protecting shared user data.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Chen *et al.* [32, 34, 35]	2005, 2011, 2013	Providing efficient and secure classifier using cloud computing technology with privacy preserved	A random space encryption (RASP) approach	Updating the encrypted database is not an easy task
Hong *et al.* [60]	2013	Preserving privacy under distributed environment	Surveying existing privacy protection strategies	Mainly focusing on time-series data mining
Dong *et al.* [41, 42]	2014, 2015	Suggesting a privacy-preserving data security policy	A series of encryption techniques	Resulting in key escrow problems
Han *et al.* [55]	2016	privacy-preserved data outsourcing under cloud environment	ABE based privacy protected data access control scheme	Requiring efficiency improvements
Le *et al.* [78]	2014	Ensuring the enforceability for multi-access to stored data in cloud servers	An inconsistency checking and removing algorithm	Requiring pre-defined rule regulations
Wang *et al.* [85, 145–147]	2011, 2013, 2014	Keeping the shared data confidential against untrusted cloud service providers	The hierarchical attribute-based encryption scheme	lacking user revocation and was restricted by the same domain condition
Rahman *et al.* [116]	2015	Protecting shared data on cloud	An information protection model combining incident handling strategy and digital forensics principles	The surveyed works were only up to the year 2014

encryption scheme [32, 34, 35], a hierarchical data-accessing scheme [55, 78, 145], and other cyber technologies [116] might be used. We believe that establishing an effective protocol in the platform is beneficial for both users and service providers. Although data analysis is necessary for service quality improvement, the part of the user data that must be revealed to the analyzer to obtain the full functionality of the sharing service remains questionable.

4.3 From the Service Provider Perspective: Making Privacy the Top Priority

As the last but important participant, the service provider has to learn the importance of protecting user privacy. Numerous studies have shown that privacy protection/security quality is an important component of the overall service quality, and therefore influences the final profit of the company [28, 131, 155]. More specifically, the enhancement of privacy protection quality by the service provider potentially attracts more

customers to pay for the service [27]. Service providers must give the privacy protection issue the highest priority in a successful business model.

Thaichon *et al.* [131] surveyed the relationships between various aspects of service quality and the perceived value by customers. They identified the four most important service quality dimensions that influence the final profit of the company, which include privacy concerns. The limitation of their work is that the survey is conducted in the context of a single country (Thailand).

Hartono *et al.* [58] further identified the most important dimensions of perceived security for online purchases as confidentiality, integrity, availability, and non-repudiation. They validated that these four aspects significantly impact the customer's willingness to participate e-commerce services by using a second-order structural model of perceived security. In their experiment, only responses from Korea were used, which may reduce the generalizability of the study results.

Ingham *et al.* [63] examined the internal relationships among trust, perceived risks and customers' acceptance in e-shopping practices. The technology acceptance model (TAM) nomological network is deeply discussed to measure the values in a different dimensions. The testing results are analyzed by the meta-analytical path approach. This was a comprehensive survey paper that searched for potential ways to promote e-commerce to achieve better sales. However, substantial techniques for enhancing the trusts gained from the customers are missing.

Wang and Lin [144] established a conceptual research framework for studying the internal links between service quality and user experience of location-based services (LBS) (Figure 12). Based on a survey with 1399 participants, Wang and Lin identified positive and negative influences between factors, such as service quality and privacy trust in using LBS. Cultural bias may be presented in their results since the survey was conducted only in Taiwan.

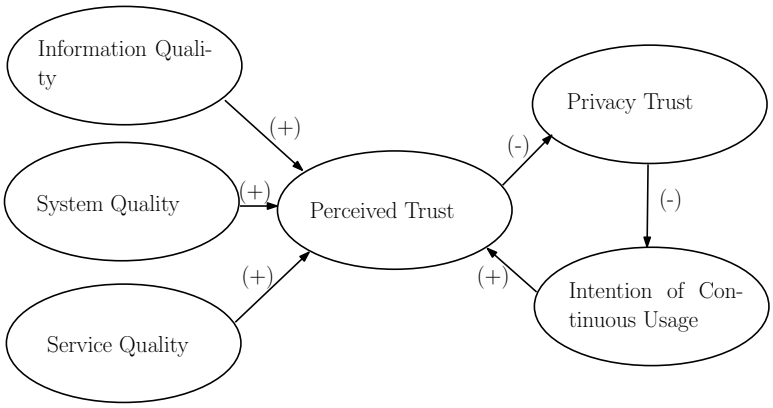

Fig. 12. The research conceptual framework proposed by Wang and Lin's studies on the relationship between various elements on service quality and the intention of continuous usage of location based services [144]. The positive and negative influences between factors are marked by '+' and '-' signs.

All surveyed works from the service providers' perspective are listed in Table 9. The internal relationship between the privacy protection and the net profit is heavily studied. Overall, the privacy protection level is an essential component in service quality evaluation and significantly impacts the customers' willingness to participate, customers' trust and net profit. Thus, it is important for the service providers to give privacy issues the top priority to improve their commercial strategies, provide a more secure servicing environment and build more successful business models.

Table 9. References, main objectives, proposed solutions and important insufficiency of the surveyed works for realizing the importance of protecting user privacy.

Reference	Year	Main objective	Proposed solution	Important insufficiency
Thaichon *et al.* [131]	2014	determining the relation between different service quality aspects (including privacy protection) and the final profit	Identifying the four most important aspects for service quality enhancement	The survey results are only limited to a single country (i.e. Thailand)
Hartono *et al.* [58]	2014	Identifying the most important dimensions of perceived security for online shopping	A second-order structural model on perceived security	Only responses from Korea are used
Ingham *et al.* [63]	2015	Examining the internal relationship between trust, perceived risks, and customers' acceptance	The technology acceptance model (TAM) nomological network	Lacking ways to gain the customers' trusts
Wang and Lin [144]	2016	Studying the internal linking of service quality and intention of continuous usage of location-based services	A research conceptual framework	The survey was only conducted in Taiwan

5 CONCLUSION, DISCUSSION AND FUTURE WORKS

In this study, we explored the main privacy concerns in sharing service practices in the current stage of the cyber-enabled world. We divided the sharing services into two categories: crowdsourcing and collaborative consumption. Each category is further divided into three branches. The resulting six branches comprehensively cover the sharing service practices in the cyber-enabled world. A substantial part of surveyed works, analyses, results and solutions were published in the recent five years, i.e., from 2013 to 2017. Figure 13 depicts the timeline statistical distribution of all listed surveyed works from Table 1 to 9.

Crowdsourcing is further divided into three branches: Internet crowdsourcing marketplace, crowdfunding and crowdtesting. In Internet crowdsourcing marketplace practices, we tackled the privacy protection problem for task requesters. Two approaches were surveyed: the coding theory and the instance clipping protocol. Various solutions for protecting the requester's privacy were proposed by extending the two approaches. In crowdfunding practices, modern crowdfunding platforms, such as Indiegogo, allow users to select their preferred security level and conceal their personal information privately, such as their names and contribution amounts. However, the surveyed works suggest that a certain level of privacy sacrifice can be helpful in crowdfunding practice. For crowdtesting practices, three real-world applications were surveyed, including shared data protection on a the cloud server [56], online surveys [69] and indoor site survey practice [81]. The main difficulties in protecting the privacy in crowdtesting practices are identified, which leads to one of the future research directions in the crowdtesting field.

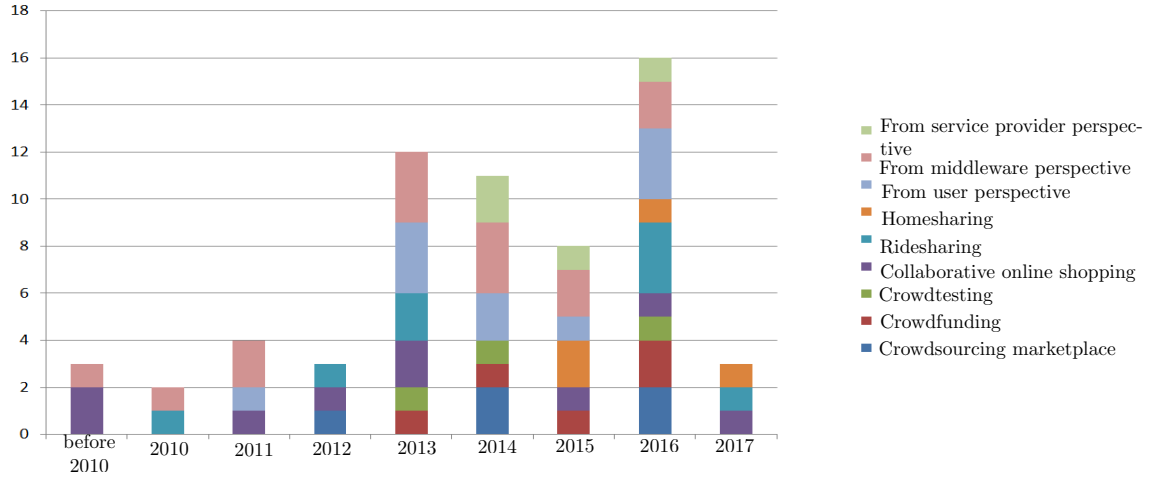

Fig. 13. The time-line statistics of all listed surveyed works from Table 1 to 9. Most surveyed works, analyses, results and solutions are from the recent five years, i.e. from 2013 to 2017.

In collaborative consumption, the three sub-categories are: collaborative online shopping, ridesharing and homesharing. Collaborative online shopping, as a new generation of online shopping experience, raises two potential privacy concerns. The first privacy concern is the misuse of user data for marketing analysis, which can be prevented by refining government regulation [113], masking customers' data before sending them out [20] or separating communication channels on the cloud server [79]. The second privacy concern is related to user awareness of privacy leakage in online shopping, which was further discussed in later sections. In ridesharing practice, it is important to note that revealing the passenger's information, such as location, is necessary for the user to utilize the service. Location privacy is heavily discussed; and we note that inter-personal interaction is a potential threat to physical privacy in ridesharing practice. For homesharing, the surveyed works reveal that the hosts are actually more concerned about their privacy leakage than the travelers. Most of the privacy concerns are physical privacy issues.

Last, we summarized the privacy concerns in the cyber-enabled sharing world from three perspectives. From the user perspective, users have started to realize that they have to sacrifice a certain degree of personal information to enjoy the sharing services. Therefore, the emerging issue is to increase the privacy awareness of the users. From the platform perspective, it is necessary for the third party platform to analyze the user's shared data to improve the service quality. The emerging issue from the platform perspective is to develop an effective protocol for identifying and protecting sensitive data during the transmission process, as well as the storage on the cloud server. From the service provider perspective, privacy must be recognized as the most important issue in the business model, which potentially impacts the perceived security and trust as well as the final profit.

In conclusion, the emerging privacy issues in the cyber-enabled world include developing a more sophisticated encryption scheme for masking the user data, a more reliable recommendation system for user privacy management, a more secure transmission protocol and etc. All these issues also represent the future research directions for privacy protection in sharing service practices.

Conflict of Interests

All authors declare that there is no conflict of interest regarding the publication of this manuscript.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China, under grant no 61602431.

REFERENCES

[1] Niels AH Agatz, Alan L Erera, Martin WP Savelsbergh, and Xing Wang. 2011. Dynamic ride-sharing: A simulation study in metro Atlanta. *Transportation Research Part B: Methodological* 45, 9 (2011), 1450–1464.
[2] Charu C Aggarwal and S Yu Philip. 2008. A general survey of privacy-preserving data mining models and algorithms. In *Privacy-preserving data mining*. Springer, 11–52.
[3] Ulrich Matchi Aïvodji, Sébastien Gambs, Marie-José Huguet, and Marc-Olivier Killijian. 2016. Meeting points in ridesharing: A privacy-preserving approach. *Transportation Research Part C: Emerging Technologies* 72 (2016), 239–253.
[4] Shahriyar Amini. 2014. Analyzing Mobile App Privacy Using Computation and Crowdsourcing. (2014).
[5] Shahrihar Amini, Jialiu Lin, Jason I Hong, Janne Lindqvist, and Joy Zhang. 2013. Mobile application evaluation using automation and crowdsourcing. (2013).
[6] Iheb Ben Amor, Salima Benbernou, Mourad Ouziri, Zaki Malik, and Brahim Medjahed. 2016. Discovering Best Teams for Data Leak-Aware Crowdsourcing in Social Networks. *ACM Transactions on the Web (TWEB)* 10, 1 (2016), 2.
[7] Susan M Andersen and Serena Chen. 2002. The relational self: An interpersonal social-cognitive theory. *Psychological Review* 109, 4 (2002), 619–45.
[8] Stephanos Androutsellis-Theotokis. 2002. A survey of peer-to-peer file sharing technologies. (2002).
[9] Nic Baddour. 2011. Indiegogo Insight: Pitch Videos Power Contributions-Increasing Them 114%. (2011).
[10] Louise Barkhuus and Anind K Dey. 2003. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns.. In *INTERACT*, Vol. 3. Citeseer, 702–712.
[11] Roberto J Bayardo and Rakesh Agrawal. 2005. Data privacy through optimal k-anonymization. In *Data Engineering, 2005. ICDE 2005. Proceedings. 21st International Conference on*. IEEE, 217–228.
[12] Russell Belk. 2010. Sharing. *Journal of consumer research* 36, 5 (2010), 715–734.
[13] Russell Belk. 2014. You are what you can access: Sharing and collaborative consumption online. *Journal of Business Research* 67, 8 (2014), 1595–1600.
[14] Russell W Belk. 1988. Possessions and the extended self. *Journal of consumer research* 15, 2 (1988), 139–168.
[15] Giampaolo Bella, Rosario Giustolisi, and Salvatore Riccobene. 2011. Enforcing privacy in e-commerce by balancing anonymity and trust. *Computers & Security* 30, 8 (2011), 705–718.
[16] Paul Belleflamme, Thomas Lambert, and Armin Schwienbacher. 2014. Crowdfunding: Tapping the right crowd. *Journal of Business Venturing* 29, 5 (2014), 585–609.
[17] Alastair R Beresford and Frank Stajano. 2003. Location privacy in pervasive computing. *IEEE Pervasive computing* 1 (2003), 46–55.
[18] Annika Bergström. 2015. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior* 53 (2015), 419–426.
[19] Claudio Bettini, X Sean Wang, and Sushil Jajodia. 2005. Protecting privacy against location-based personal identification. In *Secure data management*. Springer, 185–199.
[20] Alper Bilge and Huseyin Polat. 2013. A comparison of clustering-based privacy-preserving collaborative filtering schemes. *Applied Soft Computing* 13, 5 (2013), 2478–2489.
[21] Rachel Botsman and Roo Rogers. 2011. *What's mine is yours: how collaborative consumption is changing the way we live.* Collins London.
[22] Norman E Bowie and Karim Jamal. 2006. Privacy rights on the internet: self-regulation or government regulation? *Business Ethics Quarterly* 16, 03 (2006), 323–342.
[23] C Steven Bradford. 2012. The New Federal Crowdfunding Exemption: Promise Unfulfilled. *Securities Regulation Law Journal* 40, 3 (2012).
[24] Gordon Burtch, Anindya Ghose, and Sunil Wattal. 2013. An empirical examination of users information hiding in a crowdfunding context. In *The 34th International Conference on Information Systems (ICIS)*.
[25] Gordon Burtch, Anindya Ghose, and Sunil Wattal. 2014. An Experiment in Crowdfunding: Assessing the Role and Impact of Transaction-Level Information Controls. In *The 35th International Conference on Information Systems (ICIS)*.
[26] Gordon Burtch, Anindya Ghose, and Sunil Wattal. 2015. The hidden cost of accommodating crowdfunder privacy preferences: a randomized field experiment. *Management Science* 61, 5 (2015), 949–962.
[27] Juan Carlos Roca, Juan José García, and Juan José de la Vega. 2009. The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security* 17, 2 (2009), 96–113.
[28] Anne-Sophie Cases, Christophe Fournier, Pierre-Louis Dubois, and John F Tanner. 2010. Web Site spill over to email campaigns: The role of privacy, trust and shoppers' attitudes. *Journal of Business Research* 63, 9 (2010), 993–999.

[29] L Elisa Celis, Sai Praneeth Reddy, Ishaan Preet Singh, and Shailesh Vaya. 2016. Assignment Techniques for Crowdsourcing Sensitive Tasks. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 836–847.
[30] Nelson D Chan and Susan A Shaheen. 2012. Ridesharing in north america: Past, present, and future. *Transport Reviews* 32, 1 (2012), 93–112.
[31] Dhasarathan Chandramohan, T Vengattaraman, D Rajaguru, and Ponnurangam Dhavachelvan. 2016. A new privacy preserving technique for cloud service user endorsement using multi-agents. *Journal of King Saud University-Computer and Information Sciences* 28, 1 (2016), 37–54.
[32] Keke Chen and Shumin Guo. 2013. PerturBoost: Practical Confidential Classifier Learning in the Cloud. In *Data Mining (ICDM), 2013 IEEE 13th International Conference on*. IEEE, 991–996.
[33] Kuang Chen, Akshay Kannan, Yoriyasu Yano, Joseph M Hellerstein, and Tapan S Parikh. 2012. Shreddr: pipelined paper digitization for low-resource organizations. In *Proceedings of the 2nd ACM Symposium on Computing for Development*. ACM, 3.
[34] Keke Chen, Ramakanth Kavuluru, and Shumin Guo. 2011. Rasp: Efficient multidimensional range query on attack-resilient encrypted databases. In *Proceedings of the first ACM conference on Data and application security and privacy*. ACM, 249–260.
[35] Keke Chen and Ling Liu. 2005. Privacy preserving data classification with rotation perturbation. In *Data Mining, Fifth IEEE International Conference on*. IEEE, 4–pp.
[36] Eun-Ji Cho. 2011. Interpersonal interaction for pleasurable service experience. In *Proceedings of the 2011 Conference on designing pleasurable products and interfaces*. ACM, 68.
[37] Delphine Christin. 2016. Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software* 116 (2016), 57–68.
[38] Federal Trade Commission et al. 2012. Protecting consumer privacy in an era of rapid change. *FTC Report, Washington, DC* (2012).
[39] Neil Daswani, Hector Garcia-Molina, and Beverly Yang. 2003. Open problems in data-sharing peer-to-peer systems. In *Database TheoryICDT 2003*. Springer, 1–15.
[40] Anhai Doan, Raghu Ramakrishnan, and Alon Y Halevy. 2011. Crowdsourcing systems on the world-wide web. *Commun. ACM* 54, 4 (2011), 86–96.
[41] Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, and Minglu Li. 2014. Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing. *Computers & Security* 42 (2014), 151–164.
[42] Xin Dong, Jiadi Yu, Yanmin Zhu, Yingying Chen, Yuan Luo, and Minglu Li. 2015. SECO: Secure and scalable data collaboration services in cloud computing. *computers & security* 50 (2015), 91–105.
[43] AJ du Croix. 1985. Data sharing and access protection in Business System 12. *Computers & Security* 4, 4 (1985), 317–323.
[44] Khaled El Emam, Fida Kamal Dankar, Romeo Issa, Elizabeth Jonker, Daniel Amyot, Elise Cogo, Jean-Pierre Corriveau, Mark Walker, Sadrul Chowdhury, Regis Vaillancourt, et al. 2009. A globally optimal k-anonymity method for the de-identification of health data. *Journal of the American Medical Informatics Association* 16, 5 (2009), 670–682.
[45] Ahmed Elbery, Mustafa ElNainay, Feng Chen, Chang-Tien Lu, and Jeffrey Kendall. 2013. A carpooling recommendation system based on social VANET and geo-social data. In *Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. ACM, 556–559.
[46] Eyal Ert, Aliza Fleischer, and Nathan Magen. 2015. Trust and Reputation in the Sharing Economy: The Role of Personal Photos on Airbnb. *Available at SSRN 2624181* (2015).
[47] M Feeney. 2015. Is ridesharing safe? Cato Policy Analysis, 27 January, no. 767. (2015).
[48] Benjamin Fung, Ke Wang, Rui Chen, and Philip S Yu. 2010. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (CSUR)* 42, 4 (2010), 14.
[49] Vishal Gaikar. 2013. First eBay, Now AirBnB: The Rise of Peer to Peer Marketplaces. (2013).
[50] Sheng Gao, Jianfeng Ma, Weisong Shi, Guoxing Zhan, and Cong Sun. 2013. TrPF: A trajectory privacy-preserving framework for participatory sensing. *IEEE Transactions on Information Forensics and Security* 8, 6 (2013), 874–887.
[51] Eric Gilbert, Kathi Evans, Troy Clark, and Karl Beck. 2001. De-identification and linkage of data records. (Aug. 15 2001).
[52] MaryAnne M Gobble. 2015. Regulating Innovation in the New Economy. *Research-Technology Management* 58, 2 (2015), 62.
[53] C Graham and Robert L Goodwin Payne. 1977. Dynamic System Identification: Experiment Design and Data Analysis. *Mathematics in Science and Engineering, Academic Press, Inc* 136 (1977).
[54] Juho Hamari, Mimmi Sjöklint, and Antti Ukkonen. 2015. The sharing economy: Why people participate in collaborative consumption. *Available at SSRN 2271971* (2015).
[55] Ke Han, Qingbo Li, and Zhongliang Deng. 2016. Security and efficiency data sharing scheme for cloud storage. *Chaos, Solitons & Fractals* 86 (2016), 107–116.
[56] Hamza Harkous, Rameez Rahman, and Karl Aberer. 2014. C3p: Context-aware crowdsourced cloud privacy. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 102–122.
[57] Heinrich Hartmann, Tim Wambach, Maximilian Meffert, and Rüdiger Grimm. 2016. A privacy aware mobile sensor application. (2016).

[58] Edward Hartono, Clyde W Holsapple, Ki-Yoon Kim, Kwan-Sik Na, and James T Simpson. 2014. Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems* 62 (2014), 11–21.

[59] Johannes Heurix, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz. 2015. A taxonomy for privacy enhancing technologies. *Computers & Security* 53 (2015), 1–17.

[60] Sun-Kyong Hong, Kuldeep Gurjar, Hea-Suk Kim, and Yang-Sae Moon. 2013. A survey on privacy preserving time series data mining. In *3rd International Conference on Intelligent Computational Systems ICICS*. 44–48.

[61] Mark Hooshmand. 2015. The risks of being a host in the sharing-economy. (2015).

[62] Jeff Howe. 2006. The rise of crowdsourcing. *Wired magazine* 14, 6 (2006), 1–4.

[63] John Ingham, Jean Cadieux, and Abdelouahab Mekki Berrada. 2015. e-Shopping acceptance: A qualitative and meta-analytic review. *Information & Management* 52, 1 (2015), 44–60.

[64] Qatrunnada Ismail, Tousif Ahmed, Apu Kapadia, and Michael K Reiter. 2015. Crowdsourced exploration of security configurations. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 467–476.

[65] Priti Jagwani and Saroj Kaushik. 2012. Defending location privacy using zero knowledge proof concept in location based services. In *2012 IEEE 13th International Conference on Mobile Data Management*. IEEE, 368–371.

[66] Jamila Jefferson-Jones. 2014. Airbnb and the Housing Segment of the Modern Sharing Economy: Are Short-Term Rental Restrictions an Unconstitutional Taking. *Hastings Const. LQ* 42 (2014), 557.

[67] Hiroshi Kajino, Yukino Baba, and Hisashi Kashima. 2014. Instance-Privacy Preserving Crowdsourcing. In *Second AAAI Conference on Human Computation and Crowdsourcing*.

[68] Parves Kamal. 2016. TRUST IN SHARING ECONOMY. In *PACIS 2016 PROCEEDINGS*.

[69] Thivya Kandappu, Vijay Sivaraman, Arik Friedman, and Roksana Boreli. 2013. Exposing and mitigating privacy loss in crowdsourced survey platforms. In *Proceedings of the 2013 workshop on Student workhop*. ACM, 13–16.

[70] Minghui Kang, Yiwen Gao, Tao Wang, Haichao Zheng, and Hing Kai Chan. 2016. Understanding the Determinants of Funders Investment Intentions on Crowdfunding Platforms: A Trust-based Perspective. *Industrial Management & Data Systems* 116, 8 (2016).

[71] Vanessa Katz. 2015. Regulating the Sharing Economy. *Berkeley Technology Law Journal* 30 (2015). Issue 4.

[72] Orin S Kerr. 2003. Internet surveillance law after the USA Patriot Act: The big brother that isn't. *Available at SSRN 317501* (2003).

[73] Sabreena Khalid. 2014. Privacy Concerns in the Sharing Economy: The case of Uber. (2014).

[74] Hidetoshi Kido, Yutaka Yanagisawa, and Tetsuji Satoh. 2005. Protection of location privacy using dummies for location-based services. In *Data Engineering Workshops, 2005. 21st International Conference on*. IEEE, 1248–1248.

[75] Aniket Kittur, Ed H Chi, and Bongwon Suh. 2008. Crowdsourcing user studies with Mechanical Turk. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 453–456.

[76] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64 (2017), 122–134.

[77] Venkat Kuppuswamy and Barry L Bayus. 2014. Crowdfunding creative ideas: The dynamics of project backers in Kickstarter. *UNC Kenan-Flagler Research Paper* 2013-15 (2014).

[78] Meixing Le, Krishna Kant, and Sushil Jajodia. 2014. Consistency and enforcement of access rules in cooperative data sharing environment. *Computers & Security* 41 (2014), 3–18.

[79] Sangmin Lee, Edmund L Wong, Deepak Goel, Mike Dahlin, and Vitaly Shmatikov. 2013. πBox: A Platform for Privacy-Preserving Apps.. In *NSDI*. 501–514.

[80] Ninghui Li, Tiancheng Li, and Suresh Venkatasubramanian. 2007. t-closeness: Privacy beyond k-anonymity and l-diversity. In *2007 IEEE 23rd International Conference on Data Engineering*. IEEE, 106–115.

[81] Shujun Li, Hong Li, and Limin Sun. 2016. Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization. *EURASIP Journal on Wireless Communications and Networking* 2016, 1 (2016), 123.

[82] Yan Li, Yingjiu Li, Qiang Yan, and Robert H Deng. 2015. Privacy leakage analysis in online social networks. *Computers & Security* 49 (2015), 239–254.

[83] David A Light. 2013. Sure, you can trust us. *MIT Sloan Management Review. v43 i1* 17 (2013).

[84] Greg Little and Yu-An Sun. 2011. Human OCR: Insights from a complex human computation process. In *Workshop on Crowdsourcing and Human Computation, Services, Studies and Platforms, ACM CHI*. Citeseer.

[85] Qin Liu, Guojun Wang, and Jie Wu. 2014. Time-based proxy re-encryption scheme for secure data sharing in a cloud environment. *Information Sciences* 258 (2014), 355–370.

[86] Xueming Luo. 2002. Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management* 31, 2 (2002), 111–118.

[87] Christoph Lutz, Christian Pieter Hoffmann, Eliane Bucher, and Christian Fieseler. 2017. The role of privacy concerns in the sharing economy. *Information, Communication & Society* (2017), 1–21.

[88] Jianhua Ma. 2016. Cybermatics for Cyberization towards Cyber-Enabled Hyper Worlds. In *2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*. IEEE, 85–86.

[89] J. Ma, Kim-Kwang Raymond Choo, H. Hsu, Qun Jin, W. Liu, K. Wang, Y. Wang, and X. Zhou. 2016. Perspectives on Cyber Science and Technology for Cyberization and Cyber-enabled Worlds. In *Proc. CyberSciTech 2016 (2016 IEEE Cyber Science and Technology Congress)*.
[90] Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, and Muthuramakrishnan Venkitasubramaniam. 2007. l-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)* 1, 1 (2007), 3.
[91] Alison Macrina. 2015. The Tor browser and intellectual freedom in the digital age. *Reference & User Services Quarterly* 54, 4 (2015), 17.
[92] Delfina Malandrino, Andrea Petta, Vittorio Scarano, Luigi Serra, Raffaele Spinelli, and Balachander Krishnamurthy. 2013. Privacy awareness about information leakage: Who knows what about me?. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*. ACM, 279–284.
[93] Delfina Malandrino and Vittorio Scarano. 2011. Supportive, comprehensive and improved privacy protection for web browsing. In *Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third Inernational Conference on Social Computing (SocialCom), 2011 IEEE Third International Conference on*. IEEE, 1173–1176.
[94] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.
[95] Paul McDonald, Matt Mohebbi, and Brett Slatkin. 2012. Comparing google consumer surveys to existing probability and non-probability based internet surveys. *Google White Paper* (2012).
[96] Rene Meis and Maritta Heisel. 2016. Computer-aided identification and validation of privacy requirements. *Information* 7, 2 (2016), 28.
[97] Sandra J Milberg, Sandra J Burke, H Jeff Smith, and Ernest A Kallman. 1995. Values, personal information privacy, and regulatory approaches. *Commun. ACM* 38, 12 (1995), 65–74.
[98] Aikaterini Mitrokotsa, Cristina Onete, and Serge Vaudenay. 2014. Location leakage in distance bounding: Why location privacy does not work. *Computers & Security* 45 (2014), 199–209.
[99] Anthony D Miyazaki and Ana Fernandez. 2001. Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer affairs* 35, 1 (2001), 27–44.
[100] Ethan Mollick. 2014. The dynamics of crowdfunding: An exploratory study. *Journal of Business Venturing* 29, 1 (2014), 1–16.
[101] Robert Morgan. 2015. CYBER LIFE. (2015).
[102] Cristian Morosan and Agnes DeFranco. 2015. Disclosing personal information via hotel apps: A privacy calculus perspective. *International Journal of Hospitality Management* 47 (2015), 120–130.
[103] Jianbing Ni, Xiaodong Lin, Kuan Zhang, and X Shen. 2016. Privacy-Preserving Real-Time Navigation System Using Vehicular Crowdsourcing. In *Proc. of VTC*. 1–6.
[104] Jianbing Ni, Kuan Zhang, Xiaodong Lin, Haomiao Yang, and Xuemin Sherman Shen. 2016. AMA: Anonymous mutual authentication with traceability in carpooling systems. In *2016 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.
[105] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
[106] Patricia A. Norberg, Daniel R. Horne, and David A. Horne. 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs* 41, 1 (2007), 100–126.
[107] Inah Omoronyia, Luca Cavallaro, Mazeiar Salehie, Liliana Pasquale, and Bashar Nuseibeh. 2013. Engineering adaptive privacy: on the role of privacy awareness requirements. In *Proceedings of the 2013 International Conference on Software Engineering*. IEEE Press, 632–641.
[108] Xiao Pan, Weizhang Chen, Lei Wu, Chunhui Piao, and Zhaojun Hu. 2016. Protecting personalized privacy against sensitivity homogeneity attacks over road networks in mobile services. *Frontiers of Computer Science* 10, 2 (2016), 370–386.
[109] Xiao Pan and Xiaofeng Meng. 2013. Preserving location privacy without exact locations in mobile services. *Frontiers of Computer Science* 7, 3 (2013), 317–340.
[110] Rasananda Panda, Surbhi Verma, and Bijal Mehta. 2015. Emergence and Acceptance of Sharing Economy in India: Understanding through the Case of Airbnb. *International Journal of Online Marketing (IJOM)* 5, 3 (2015), 1–17.
[111] Charith Perera, Rajiv Ranjan, and Lizhe Wang. 2015. End-to-End Privacy for Open Big Data Markets. *IEEE Cloud Computing* 2, 4 (2015), 44–53.
[112] Yves Poullet. 2006. EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review* 22, 3 (2006), 206–217.
[113] Sören Preibusch, Thomas Peetz, Gunes Acar, and Bettina Berendt. 2016. Shopping for privacy: Purchase details leaked to PayPal. *Electronic Commerce Research and Applications* 15 (2016), 52–64.
[114] pybossa. 2015. PYBOSSA. (2015). pybossa.com.
[115] Hannah Quay-de la Vallee, Paige Selby, and Shriram Krishnamurthi. 2016. On a (Per) Mission: Building Privacy Into the App Marketplace. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, 63–72.
[116] Ab Rahman, Nurul Hidayah, and Kim-Kwang Raymond Choo. 2015. A survey of information security incident handling in the cloud. *Computers & Security* 49 (2015), 45–69.
[117] Leah Muthoni Riungu, Ossi Taipale, and Kari Smolander. 2010. Research issues for software testing in the cloud. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on*. IEEE, 557–564.

[118] Anam Sajid and Haider Abbas. 2016. Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. *Journal of medical systems* 40, 6 (2016), 1–16.
[119] Pierangela Samarati. 2001. Protecting respondents identities in microdata release. *IEEE transactions on Knowledge and Data Engineering* 13, 6 (2001), 1010–1027.
[120] Pierangela Samarati and Latanya Sweeney. 1998. Generalizing data to provide anonymity when disclosing information. In *PODS*, Vol. 98. 188.
[121] Juliet Schor. 2014. Debating the sharing economy. *essay published by the Great Transition Initiative, Tellus Institute, available at http://www. greattransition. org* (2014).
[122] Siamak F Shahandashti, Reihaneh Safavi-Naini, and Nashad Ahmed Safa. 2015. Reconciling user privacy and implicit authentication for mobile devices. *Computers & Security* 53 (2015), 215–233.
[123] Wen Shen, Alanoud Al Khemiri, Abdulla Almehrezi, Wael Al Enezi, Iyad Rahwan, and Jacob W. Crandall. 2017. Regulating Highly Automated Robot Ecologies: Insights from Three User Studies. In *Proceedings of the Fifth International Conference on Human-Agent Interaction (HAI 2017)*. ACM, 111–120.
[124] Wen Shen and Cristina Lopes. 2015. Managing Autonomous Mobility on Demand Systems for Better Passenger Experience. In *International Conference on Principles and Practice of Multi-Agent Systems*. Springer, 20–35.
[125] Wen Shen, Cristina V Lopes, and Jacob W Crandall. 2016. An online mechanism for ridesharing in autonomous mobility-on-demand systems. In *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*. AAAI Press, 475–481.
[126] Wen-Lung Shiau and Margaret Meiling Luo. 2012. Factors affecting online group buying intention and satisfaction: A social exchange theory perspective. *Computers in Human Behavior* 28, 6 (2012), 2431–2444.
[127] Reza Shokri, George Theodorakopoulos, and Carmela Troncoso. 2016. Privacy games along location traces: A game-theoretic framework for optimizing location privacy. *ACM Transactions on Privacy and Security (TOPS)* 19, 4 (2016), 11.
[128] Jeremy Snyder. 2016. Crowdfunding for medical care: ethical issues in an emerging health care funding practice. *Hastings Center Report* 46, 6 (2016), 36–42.
[129] B Sullivan. 2002. Ebay Privacy Policy Draws FireAgain. *Computerworld, March* 20 (2002).
[130] Latanya Sweeney. 2002. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 05 (2002), 557–570.
[131] Paramaporn Thaichon, Antonio Lobo, Catherine Prentice, and Thu Nguyen Quach. 2014. The development of service quality dimensions for internet service providers: Retaining customers of different usage patterns. *Journal of Retailing and Consumer Services* 21, 6 (2014), 1047–1058.
[132] Hien To, Gabriel Ghinita, and Cyrus Shahabi. 2014. A framework for protecting worker location privacy in spatial crowdsourcing. *Proceedings of the VLDB Endowment* 7, 10 (2014), 919–930.
[133] Janice Y Tsai, Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* 22, 2 (2011), 254–268.
[134] Özlem Uzuner, Yuan Luo, and Peter Szolovits. 2007. Evaluating the state-of-the-art in automatic de-identification. *Journal of the American Medical Informatics Association* 14, 5 (2007), 550–563.
[135] Debra A Valentine. 2000. Privacy on the Internet: The evolving legal landscape. *Santa Clara Computer & High Tech. LJ* 16 (2000), 401.
[136] Lav R Varshney. 2012. Privacy and reliability in crowdsourcing service delivery. In *2012 Annual SRII Global Conference*. IEEE, 55–60.
[137] Lav R Varshney, Aditya Vempaty, and Pramod K Varshney. 2014. Assuring privacy and reliability in crowdsourcing with coding. In *Information Theory and Applications Workshop (ITA), 2014*. IEEE, 1–6.
[138] Aditya Vempaty, Yunghsiang S Han, Lav R Varshney, and Pramod K Varshney. 2014. Coding theory for reliable signal processing. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*. IEEE, 200–205.
[139] Aditya Vempaty, Lav R Varshney, and Pramod K Varshney. 2014. Reliable crowdsourcing for multi-class labeling using coding theory. *IEEE Journal of Selected Topics in Signal Processing* 8, 4 (2014), 667–679.
[140] Idalides J Vergara-Laurens, Luis G Jaimes, and Miguel A Labrador. 2017. Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. *IEEE Internet of Things Journal* 4, 4 (2017), 855–869.
[141] Hans Vertommen. 1980. The structure and conformity of meaning of interpersonal behaviors in different forms of relationships. *Rev.colomb.cardiol* 20, 5 (1980), 287–299.
[142] Kim-Phuong L Vu and Robert W Proctor. 2016. User Privacy Concerns for E-Commerce. (2016).
[143] Maja Vuković. 2009. Crowdsourcing for enterprises. In *Services-I, 2009 World Conference on*. IEEE, 686–692.
[144] Edward Shih-Tse Wang and Ruenn-Lien Lin. 2016. Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. *Behaviour & Information Technology* (2016), 1–9.
[145] Guojun Wang, Qin Liu, Jie Wu, and Minyi Guo. 2011. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. *Computers & Security* 30, 5 (2011), 320–331.
[146] Guojun Wang, Qin Liu, Yang Xiang, and Jianer Chen. 2014. Security from the transparent computing aspect. In *Computing, Networking and Communications (ICNC), 2014 International Conference on*. IEEE, 216–220.

[147] Guojun Wang, Fengshun Yue, and Qin Liu. 2013. A secure self-destructing scheme for electronic data. *J. Comput. System Sci.* 79, 2 (2013), 279–290.

[148] Haoyu Wang, Jason Hong, and Yao Guo. 2015. Using text mining to infer the purpose of permission use in mobile apps. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 1107–1118.

[149] Tsang-Yi Wang, Yunghsiang S Han, Pramod K Varshney, and Po-Ning Chen. 2005. Distributed fault-tolerant classification in wireless sensor networks. *IEEE Journal on Selected Areas in Communications* 23, 4 (2005), 724–734.

[150] Yang Wang, Yun Huang, and Claudia Louis. 2013. Respecting user privacy in mobile crowdsourcing. *SCIENCE* 2, 2 (2013), pp–50.

[151] Adrian Wright. 2001. Controlling risks of E-commerce Content. *Computers & Security* 20, 2 (2001), 147–154.

[152] Lin Yao, Chi Lin, Xiangwei Kong, Feng Xia, and Guowei Wu. 2010. A clustering-based location privacy protection scheme for pervasive computing. In *Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing*. IEEE Computer Society, 719–726.

[153] Georgios Zervas, Davide Proserpio, and John Byers. 2014. The rise of the sharing economy: Estimating the impact of Airbnb on the hotel industry. *Boston U. School of Management Research Paper* 2013-16 (2014).

[154] Tao Zhang, Jerry Gao, and Jing Cheng. 2017. Crowdsourced Testing Services for Mobile Apps. In *Service-Oriented System Engineering (SOSE), 2017 IEEE Symposium on*. IEEE, 75–80.

[155] Y Lisa Zhao and C Anthony Di Benedetto. 2013. Designing service quality to survive: Empirical evidence from Chinese new ventures. *Journal of Business Research* 66, 8 (2013), 1098–1107.

[156] Haichao Zheng, Jui-Long Hung, Zihao Qi, and Bo Xu. 2016. The role of trust management in reward-based crowdfunding. *Online Information Review* 40, 1 (2016), 97–118.

[157] Hengshu Zhu, Hui Xiong, Yong Ge, and Enhong Chen. 2014. Mobile app recommendations with security and privacy awareness. In *Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 951–960.