Emerging Privacy Issues in Cyber-Enabled Sharing Services: Survey and Solutions

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

The development of sharing services is 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 the perspectives of both users and service providers. 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 two perspectives, namely, the user perspective and service provider perspective.

CCS Concepts: •**General and reference** → *Surveys and overviews;* •**Security and privacy** → *Security services; Privacy protections;*

Additional Key Words and Phrases: Cyber Technology, Sharing Service, Privacy, Crowdsourcing, Collaborative Consumption

ACM Reference format:
Ke Yan, Wen Shen, Huijuan Lu, and Qun Jin. 2016. Emerging Privacy Issues in Cyber-Enabled Sharing Services: Survey and Solutions. 1, 1, Article 1 (January 2016), 31 pages.
DOI: 10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Cyberization is transforming our physical living world into a virtual computerized world by leveraging Internet and computational methodologies [82, 83]. In the virtual computerized world, or more specifically the cyber-enabled world, people are connected through the Internet regardless of their physical distance. Traditional businesses and services, such as transportation, accommodation, shopping, entertainment and etc, tend to either completely migrate to an online mode or at least build an online presence. Online

This work is supported by the National Natural Science Foundation of China, under grant 61602431.
Author's addresses: K. Yan and H. Lu, College of Information Engineering, China Jiliang University, 258 Xueyuan Street, Hangzhou, China, 310018; W. Shen, Department of Informatics, University of California Irvine, Irvine, CA 92697; Q. Jin, Department of Human Informatics and Cognitive Sciences, Waseda University, 2-579-15 Mikajima, Tokorozawa-shi, Saitama 359-1192, Japan.

DOI: 10.1145/nnnnnnn.nnnnnnn

service companies are recognized as components of the cyber-enabled world that promote cyber life-style using cyber technologies. These cyber-life companies have been receiving overwhelming popularity and enjoying incredible growth over the past few years, which include popular company names, e.g. Uber, Airbnb, Esty and Amazon Family Library [11, 95, 138].

Cyber-enabled sharing services, or in short, sharing services, which provide information, goods and services in a shared form to multiple individuals, knowing or not knowing each other, is an essential and necessary step in cyber world development and probably the most exciting cyber related concept in the current stage of cyberization. Sharing services encourage people to share virtual or physical assets through internet and client devices, such as computers and mobile phones. They contribute to the fast development of the cyber technology, where the control, responsibility for the common good, earnings, capitalization, information and efforts are all shared with the participants or distributed to peer members [112]. For instance, there is no single entity or person can control the whole market or economy, though some participants have more regulatory power than the others. All participants share the responsibility of making the market operate healthily. This form of collaborative economy or peer-to-peer (P2P) sharing brings more efficient allocation of resources and builds more sustainable future life for the cyber-enabled world.

There are various reasons for people to participate in sharing practices. The most important one is that users are able to get their demands satisfied in an efficient or economic way through sharing. For example, if a person needs a ride to a mall, he/she may simply use a P2P car sharing service such as Uber or Lyft. Obviously, it is more convenient to use the mobile app to order a ride service on demand compared to the traditional phone-booking service while he/she has the uncertainty about the future travel plan. Moreover, it is usually cheaper to use the P2P car sharing service. However, in order to attract more people to share, it is necessary to build trust, establish reputation, protect privacy and guarantee security of the participants [12]. Personal privacy is the major factor that hinders the development of the sharing services in the cyber-enabled world [37, 40]. On one hand, people are reluctant to adopt sharing practices because of the concern of privacy leakage or disclosure [44, 51, 77]; on the other hand, sharing service providers insist that the personal data is part of the necessary information in user experience analysis to improve the service quality. While only privacy protection is explored in this paper, authors argue that privacy is relevant and closely related to trust, reputation and security. First, users need to trust the service provider, which implies that the service provider should have a good reputation that the users can trust. Both the service provider and the users establish reputations through interaction with each other. Second, during the interaction, privacy issues arise while information from both parties are revealed to each other.

In this study, we point out the emerging privacy issues of the sharing services in the cyber-enabled world and review available solutions in detail. From the literature, we summarize the sharing services in the current stage of cyber-enabled world into two categories [20, 112]:

- **Crowdsourcing** employs collective intelligence or power to fulfill tasks or achieve goals. The concrete examples of crowdsourcing are Internet crowdsourcing marketplace, crowdfunding and crowdtesting.
- **Collaborative consumption** allows consumers to use the products or services without full ownership. The concrete examples of the collaborative consumption include: collaborative online shopping, ridesharing and homesharing practices.

The review of privacy issues and solutions follows the above two routines and reveal the main concerns in the literature, which include the requester's data protection, the user's identity protection, financial information disclosure, transaction protocols, testing product details protections, user agreement terms

on privacy, location privacy and personal privacy. Figure 1 lists a taxonomy of the paper surveyed in this study.

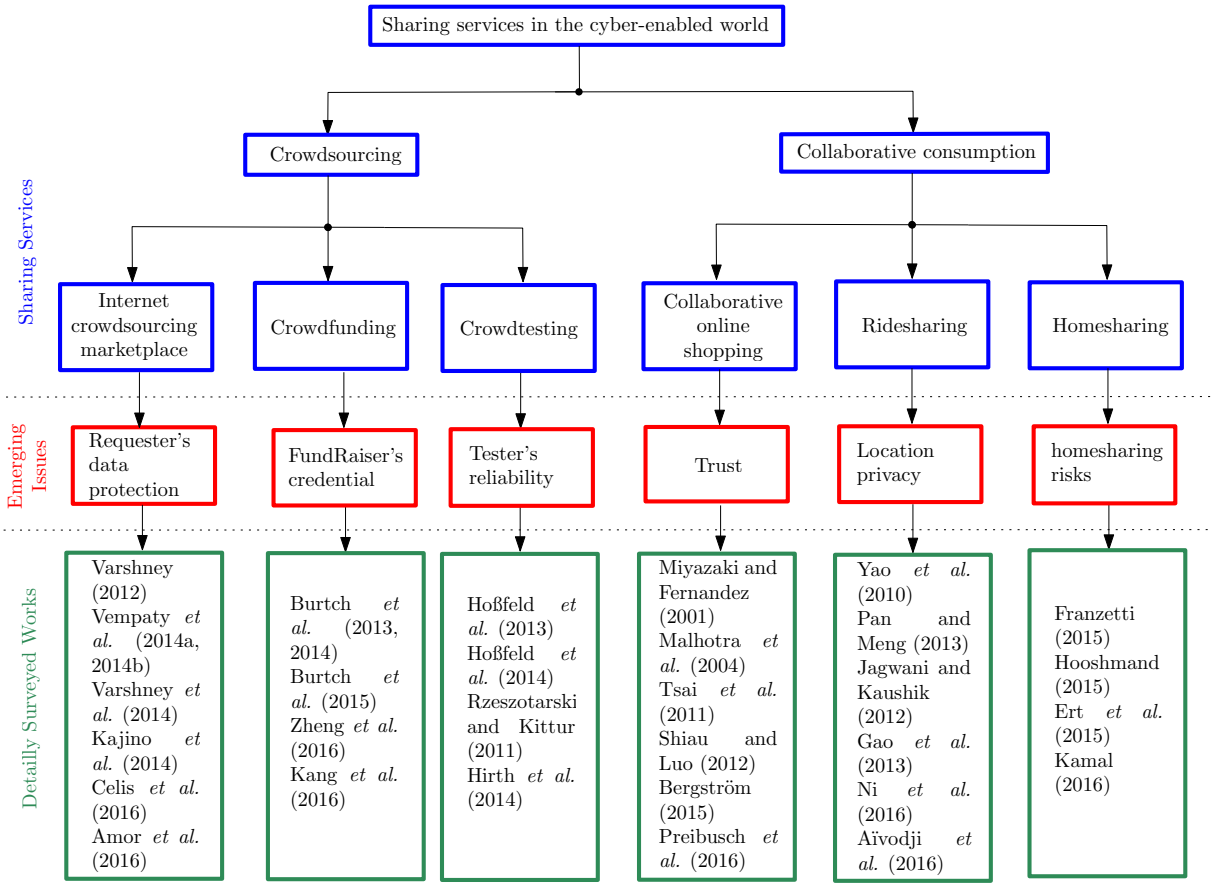

Fig. 1. Taxonomy of sharing services in the cyber-enabled world (in blue rectangles), identified emerging privacy issues (in red rectangles) and surveyed works in the literature (in green rectangles)

Although there are similar works about privacy concern in sharing practices from the literature, e.g. [2, 7, 46, 57, 107], they focused on traditional privacy protection methods, such as the k-anonymity [117], l-diversity [84] and t-closeness [76]. In contrast, our work focuses on the privacy protection technique development in the recent five years, skips the traditional approaches and covers technologies comprehensively in the area of cyber-enabled sharing services. Most surveyed works in this study are selected from the year 2011 to the year 2016. The sources of the reviewed papers include the most popular databases, such as Google Scholar, IEEE Xplore Digital Library, Springer Link and ScienceDirect. The searched keywords include 'sharing service', 'privacy issue', 'privacy protection', 'crowdsourcing privacy', 'collaborative consumption privacy', 'crowdfunding privacy' and etc.

The paper is organized as follows: the emerging privacy issues and solutions of crowdsourcing are analyzed in detail in Section 2. The emerging privacy issues and solutions of the collaborative consumption are reviewed in Section 3. In Section 4, we summarize all the privacy issues in Sections 2 and 3 from user,

middleware and service provider perspectives. In Section 5, several conclusions are drawn for the cyber technology development to show the future trends of developing cyber-enabled sharing technologies.

2 PRIVACY ISSUES AND SOLUTIONS IN CROWDSOURCING PRACTICES

Crowdsourcing is a concept that allows us to outsource tasks to a large group of people from an online community, rather than from employees or service providers [63] (Figure 2). Crowdsourcing are frequently used to solve problems that are difficult or impossible for an individual to solve. Despite of its many advantages, crowdsourcing brings increasing risks of information leakage and privacy violation, which limits the advance of its development and use potential.

There are two types of users in a crowdsourcing platform: the worker (or the employee) and the requester (or the employer). The 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 of them 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 marketplace, crowdfunding, and crowdtesting. In each application, we figure the privacy protection issue in the process of sharing practice and survey the existing solution in the literature.

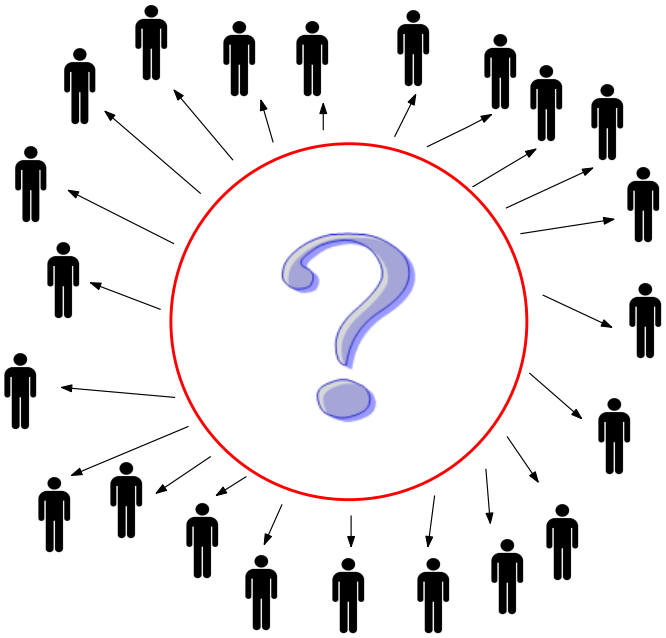

Fig. 2. Crowdsouring

2.1 Crowdsourcing Marketplace

Online crowdsourcing marketplace provides a platform to bridge the task requesters and the task performers for mutual benefits. Numerous crowdsouring marketplaces have been developed during the

past few years. Among them, Amazon Mechanical Turk (MTurk) [73] is the most notable one. MTurk enables individuals and business entities to use human intelligence to perform tasks that are difficult or impossible for computers to do automatically at present. Requesters post jobs or work as the form of human intelligence tasks on the MTurk platform, while workers then can browse the existing tasks and complete them to earn monetary incentives from the requesters.

Data privacy concerns limit the speed of spreading crowdsourcing because users refuse to participate in crowdsourcing if data is not securely protected. For example, when a requester evaluates the design of a particular artifact, it is likely that the requester desires to keep the artifact unexposed to others. Similarly, a testing organization usually requires test takers not to disclose the content of the test. However, unlike the testing organization who has the power to penalize the test takers who violates the confidentiality agreements, the requester does not always have the power or effective methods to penalize the workers who leak the sensitive data or extract the 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.

There are generally two approaches to tackle the privacy protection problem for the requesters. The first approach is known as the coding theory which was originally proposed by Varshney in 2012 [123]. A set of random perturbations are added to the requester's data, especially for the sensitive part, in order to conceal the private information from the workers. They used a mathematical model to generate the random perturbation, and named the method as coding theory. A series of extensions are introduced by the same group of researchers to complete the framework by considering the privacy-reliability problems [125, 126]. The coding theory successfully hides the sensitive information from the workers. However, it loses the task performance quality while random perturbations are added to the original data. In 2014, Varshney *et al.* [124] studied the tradeoffs between privacy, reliability, and cost. The coding scheme is further improved by considering five insight elements, namely error correcting codes, reliability, perturbation, decoding and collusion attacks.

The second approach is the instance clipping protocol (ICP) which was first learned by Little and Sun [79] and Chen *et al.* [32]. 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 defined as contextual information. The instance-privacy preserving protocols preserves 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 task result. The ICP preserves privacy while it may decrease the quality of the task results. Similar to Varshney's work, trade-offs exist to balance the privacy preserving and task quality. The instance clipping protocol clips an instance by a moving window, which preserves the data privacy by limiting the data that worker acquires.

Celis *et al.* [28] improved the clipping protocol by a collusion network. In a collusion network, the requesting task can be partitioned to different workers with minimal privacy leaks. Moreover, a crowdsourcing framework is proposed with three operations: PULL, PUSH and Tug Of War (TOW). The PULL and PUSH are two usual operations which represent worker choosing tasks and requester choosing workers respectively. The TOW is an intermediate layer which is built in the system to minimize the information leakage. Discussions are raised while the TOW operation takes the worker's personal information into account, 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' to managing the competition and collaboration in crowdsourcing process. The SocialCrowd system deeply analyzes the social relationship of the workers and organizes them based on clustering algorithms. Experimental results showed that the data leakage

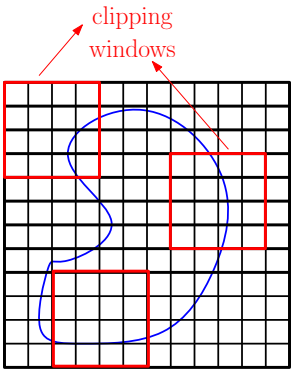

Fig. 3. Instance clipping protocol.

was effectively prevented and the efficiency of the crowdsourcing task was increased. The main concern of Amor *et al.*'s work was the time complexity, since the optimal solution could be found only by searching the whole space. One solution proposed by the authors was to use a heuristic random search algorithm which could be risky for local minima or maxima.

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 [123]	2012	Concealing the requesters' information from the workers	A basic coding theory	Not considering the privacy-reliability problem
Vempaty *et al.* [125, 126]	2014	Generalizing the coding theory in [123]	A more completed framework for the coding theory	Losing the task performance quality
Varshney *et al.* [124]	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.* [28]	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

In summary, Table 1 listed all references that we have discussed in this section, including their main objectives, proposed solutions and possible weaknesses. While the traditional works focus on protecting the requesters' data in a fundamental way, more issues are raised to improve the user awareness of the privacy leakage during the crowdsourcing practice, which will be discussed in Section 4.1.

2.2 Crowdfunding

Crowdfunding gains fast development recently [13, 94]. It enables founders of various ventures to fund their projects by collecting fund or other resources from a large group of individuals through an online platform such as such as Kickstarter [74] and Indiegogo [8]. While most research focuses on the economic aspects of crowdfunding, few addresses the privacy issues in it [22]. To bridge the gap, we hereby discuss the privacy protection problems and solutions in crowdfunding.

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 to the project. The investment decision is made with payments as well as personal information, such as names, contact numbers, and addresses, revealed to both the platform and the fundraiser. The user also has to reveal the financial information such as banking account or credit card information to the platform. All these sensitive information must be securely protected. Data leakage of such information may result in financial loss or even endangerment of personal safety [113].

While crowdfunding platforms usually guarantee the security of the transactions, they generally do not check the credentials of the fundraisers. Some unqualified fundraisers gather user data for other purposes (e.g., data analysis for advertisements). These fundraisers usually are not committed to fulfill the projects they propose. However, current mechanisms or protocols do not prohibit fundraisers from collecting user data no matter their projects succeed or fail. Therefore, it is important for the platforms to evaluate the credentials of the fundraisers and institute privacy protection related policies (similar to the market-access policies in international trade). Recent studies also reveal the fundraiser's credential problem in the crowdfunding practices. Ying [137] reviewed the crowdfunding regulations in Singapore and pointed out the risks behind of wiring money to low-reputable fundraisers.

Burtch *et al.* [23, 24] conducted a series of experiment on a large-scale crowdfunding platform to test the relationship between the security setup and the willingness of contribution for users. An econometric model was constructed where the dependent variables included the likelihood of information hiding and the amount of contribution from crowdfunders. The independent variables included the privacy control of the fundraiser's platform, elapsed time of fundraising, fundraiser's reputation and etc. Six hypotheses were formulated, including 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 shown in 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.* [25] conducted another online experiment to study the hidden cost of protecting crowdfunders's privacy utilizing modern techniques, such as invisible transaction information. Their result pointed out that the privacy protection in overall increased the net funding that was composed by two competing influences: increasing of willingness to engage with the crowdfunding (a 4.9% increment of willingness in average) and decreasing of average contribution (a $5.8 decrement). Their finding revealed the importance of implementing privacy protection mechanisms in the crowdfunding platform. The main

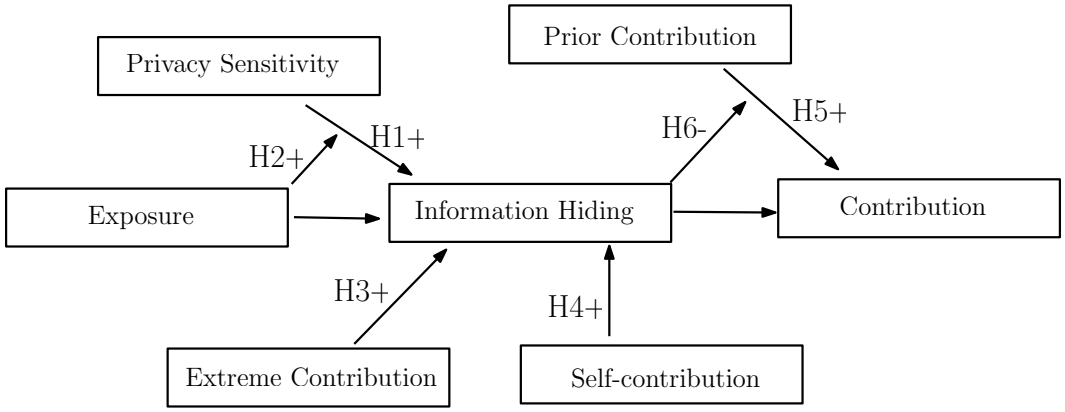

Fig. 4. The econometric model proposed by Burtch *et al.* [23, 24].

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 experiment result unreliable.

Zheng *et al.* [140] analyzed the importance of trust management in the practice of crowdfunding. They constructed a research model, which was based on the elaboration likelihood model (ELM), to test five hypotheses that they made. Experiemtal results showed that effective trust management techniques significantly improve the fundraising performance. Moreover, they found that the prior success fundraising records positively promote the entrepreneur-sponsor interaction in crowdfunding practices. Limitation existed while the study only focused on the trust management and ignored other highly influential factors, such as the funding information and presentation format in the funding description.

Kang *et al.* [69] proposed a structural equation modeling technique to reveal the 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 trustfulness of a crowdfunding project. The fundraiser's credentials are analyzed by bootstrapping method based on the historical investment experiences. However, their conclusion was draw based on a small sized survey dataset in scope to only one country, which was lack of validations via cross-sectional survey methods.

We summarize the reviewed works for privacy issues in crowdfunding practices in Table 2. Each reviewed work is accompanied with its reference, year, main objective, proposed solution and important insufficiency. As the crowdfunding is relatively a new concept to people in the cyber-enabled world and directly assets related, information security issues are more emerging and considered as important research topics in the development process of cyber-enabled world.

2.3 Crowdtesting

Crowdtesting employs crowsourcing and cloud platforms to find potential testers to test software or products. The requesters post their testing tasks on the web. The testers pick up 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 [108, 128]. An example of crowdtesting is PyBossa [106] which offers open source platform for customized crowdsourcing tasks that require human cognition, knowledge or intelligence. The objectives of a crowdtesting can be the testing of usability, acceptability, task performance and the users overall quality of experience (QoE). In the cyber-enabled

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.* [23, 24]	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.* [25]	2015	Showing the hidden cost of protecting crowdfunders's privacy utilizing modern techniques	Online randomized experiments	Experiment users are given complete freedom for their fund contributions
Zheng *et al.* [140]	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.* [69]	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

world, the crowdtesting main focuses on the QoE of web services, such as online TV, video games, web-based phone call services, video conferences and etc.

The privacy concern involved in the crowdtesting practice is that the testers may reveal their testing results from one to another. Interestingly, unlike other sharing practices discussed in this study, such as the crowdsourcing marketplace and crowdfunding, testers usually do not care about revealing the testing results from one to another, although they may easily understand that the results are part of their privacy. The behavior of sharing results offends both privacy protection practices of the testers and the requester. Therefore, efforts have to be made to detect and consequently prevent the sharing behaviors.

Rzeszotarski and Kittur [109] first proposed implicit behavioral measures to detect low-quality submissions of testing results in crowdtesting practices. They offered an interesting thought: focusing on the way that a tester works instead of only examining the testing result. Based on Rzeszotarski and Kittur's idea, Hirth *et al.* [58] predicted the quality of a testing result by a method called application layer monitoring. They compared the tester's behavior during the testing process with an expected behavior model designed in the system. The expected behavior model was constructed by machine leaning technology based on a set of training dataset containing past testers' behaviors. Both works focus on dishonest behavior detection and do not propose any protocols to prevent those behaviors.

Hoßfeld *et al.* [61, 62] had a detailed discussion about the key issues in the development process of crowdtesting and proposed numerous remedies to the design, implementation and reliability assessment for the crowdtesting practices. Fundamentally, the crowdtesting process is an unsupervised working scenario. It is more convenient for the testers to obtain the testing results from others instead of reading tedious online documents in order to claim the payoff efficiently. The proposed crowtesting scheme discouraged the testers to share their testing results and prompted them to understand that the results are part of their own and the requester's privacy. It is one step further; but the most effective crowdtesting scheme

to prevent cheating, make the testing results more reliable as well as protecting the privacy is still left for future exploring.

To conclude, there are not much works in the crowdtesting field concerning about the privacy issue. More existing works only focus on the test quality measurement [93]. However, we would like to point out that without proper privacy protection scheme, the crowdtesting results can never be reliable. A summary of the main privacy concerns and solutions proposed by reviewed works are listed in Table 3.

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

Reference	**Year**	**Main objective**	**Proposed solution**	**Important insufficiency**
Rzeszotarski and Kittur [109]	2011	Examining the ways that testers' works	Implicit user behavioral measures	Low detection rate on dishonest behavior
Hirth *et al.* [58]	2014	Learning past testers' behaviors	Application layer monitoring method	Lack of techniques to prevent cheating
Hoßfeld *et al.* [61, 62]	2013, 2014	Making the QoE crowdtesting reliable	Numerous remedies to the design, implementation and reliability assessment for crowdtesting	The most effective crowdtesting scheme to prevent cheating is still left for further exploring

2.4 Summary and Discussion

In crowdsourcing practices, the requester has the responsibility to protect workers' data privacy. On one hand, the requester should not disclose or misuse user data to third parties without the consents of the workers. On the other hand, the requester should design mechanisms or protocols to discourage workers to leak sensitive data of the tasks. The workers are responsible to follow the privacy agreements of tasks. The platform serves as a mediator to protect the privacy of both parties. There are always trade-offs between privacy and interests (e.g., incentives, task quality, funds).

In general, for a crowdsourcing platform, users should be allowed to retrieve information from the database of a sharing service provider while the queries are maintained privately. Gertner *et al.* [49] introduced a model of symmetrically-private information retrieval (SPIR), which protects the privacy of the data and that of the user. This method facilitates the implementation of communication efficient SPIR schemes, which requires only one round of interaction and withstands any dishonest behavior of the user.

To reconcile the demand of data releasing for research purposes and the demand of data privacy for users, data de-identification methods have been proposed and widely used [41, 50, 52, 121]. In addition, traditional methods, such as $k-$anonymity and $l-$diversity models, can be used to avoid linking attacks while the integrity of the released data is preserved [10, 111].

3 PRIVACY ISSUES AND SOLUTIONS IN COLLABORATIVE CONSUMPTION PRACTICES

Unlike crowdsourcing which collects the power of individuals to perform tasks, collaborative consumption allows individual to access goods or services through P2P sharing, which is coordinated by online services [11, 18]. Collaborative consumption has many benefits such as reducing greenhouse gas emissions,

saving costs, providing access to unaffordable goods, and increasing independence, flexibility by decentralization [17, 53]. Typical examples of collaborative consumption include collaborative online shopping websites such as eBay, Craigslist as well as ridesharing (Uber) and homesharing (Airbnb) (Figure 5). Although collaborative consumption has many advantages, it suffers from privacy concerns which limit its development. In this section, we review problems and solutions of privacy protection in collaborative consumption.

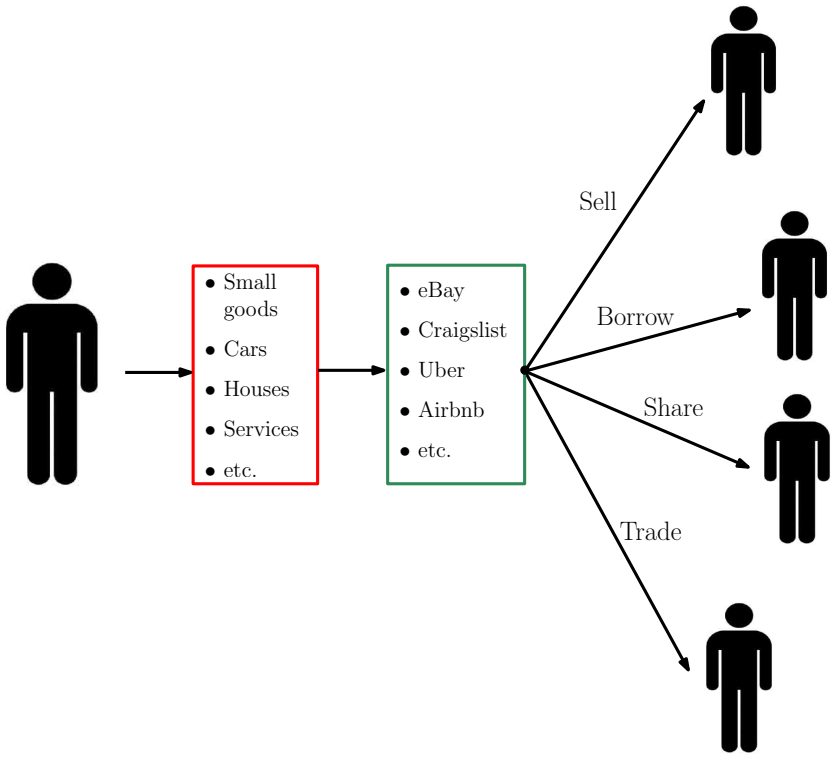

Fig. 5. Collaborative consumption.

3.1 Collaborative Online Shopping

Online shopping is probably the first successful model to show that the cyber technology has been changing our living world. In the first stage of online shopping development, people found that it is more convenient and economic to purchase goods from the Internet. In the process of cyber technology development, the concept of collaborative consumption is gradually embedded into the online shopping experience. People started to sell small stuffs, trade services, share cars and borrow things through the online shopping websites [19].

On the other hand, the online shopping websites have received many criticisms due to their notorious privacy polices despite of their popularity [21, 78, 116, 122, 135]. Although it is illegal to reveal user information to third parties without user consents, the online platforms are not subject to penalty for analyzing user data. These platforms may rely on third-party organizations for data analysis, which might

deteriorate users' privacy. However, in order to use the services, users have no choice but to accept the privacy policy terms without negotiations, which is unfair to users. In fact, except for limited government regulations, these marketplaces are self-regulated or autonomous, making 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 [92] conducted a survey about online shopping fears on a set of U.S. Internet users with different age groups, economical classes, educational background. The survey results indicated that the untrusted security system is the biggest fear for the customers. Malhotra *et al.* [88] systematically analyzed the Internet users' information privacy concerns (IUIPC) through two separate surveys from 742 household respondents. They designed a theoretical framework to study the IUIPC and proposed a causal model that predicts the reaction of online customers to privacy threats from the shopping websites. Tsai *et al.* [120] studied how the privacy concerns of customers affect their decisions in the online shopping process. They conducted an experiment to test the shopping decision made by customers after displaying their personal information on the shopping websites. The results showed that the customers were actually willing to pay an extra premium to purchase goods from a more privacy protective shopping website. All above mentioned survey works reveal the fact that the privacy concern is the main fear for online shopping experiences. However, these works do not do deep analysis for how to build the privacy protection trust between the online shopping websites and the customers.

Shiau and Luo [115] built a research model using partial least squares (PLS) analysis to indicate the relationship between consumer satisfaction, intension of online group buying and user beliefs (Figure 6). The PLS analysis results show that the consumer satisfaction highly replies on the trust, followed by reciprocity. It is the first work drawing an overall picture for different factors affecting the online shopping decision. Moreover, it is also the first work clearly pointing out the privacy concern is the first prioriy for online shopping security. Following Shiau and Luo's work, Bergström [15] built a analytic system with different groups of people concerning various privacy issues in online shopping experiences. Both the users and privacy concerns are partitioned into detailed dimensions to interpret the relationship between socialization, Internet experience, trust, politics and the understanding of privacy concern. Their analysis result clearly points out that the trust is the major concern of people worrying about misuse of personal data. Although these research models are one more step further than the simple survey results, it still lacks of a clear solution for protecting the online customers' privacy.

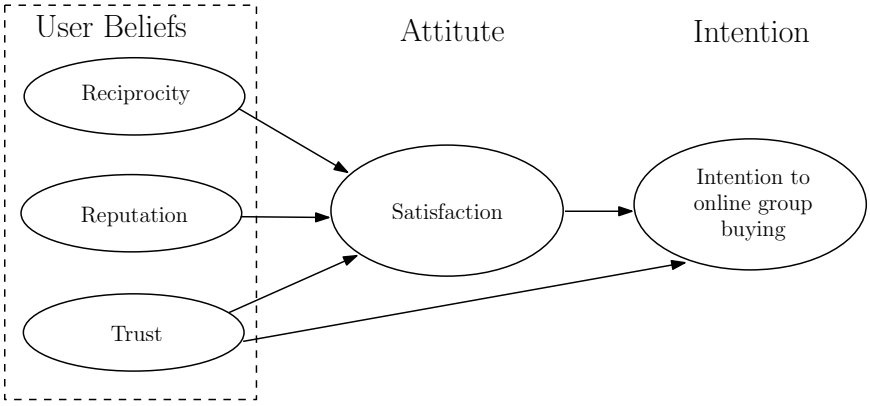

Fig. 6. The research model proposed by Shiau and Luo [115].

Preibusch *et al.* [105] studied and reported a concrete example of the privacy leakage in online shopping practices. They performed an online tracking and found that the online shopping websites send unnecessary personal information to payment providers, such as Paypal. Therefore, there is on-going danger for customers to do shopping online. The most effective method to change this situation is to facilitate relevant legislation. However, the lack of government regularization of online shopping websites exists globally. And what rules to be added and how to add are two big questions left out. Although there are existing regulations, such as the Directive 95/46/EC by the European Union [104] and the USA Patriot Act [70], 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 protective software to the web-browser. Available software on the internet includes the Tor Browser [85], the Privacy Bird [127], the Platform for Privacy Preferences [103]. These third-party software pieces or plugins identify untrusted shopping websites and mask personal information for the users. However, third-party software is usually not formally authorized or registered from the local government, which potentially raises other concerns of privacy leakage.

All reviewed works (Table 4) show that the most effective solution for online shopping privacy protection is still arguable. We point out that the privacy protection problem can be viewed from other aspects, such as raising the privacy awareness of users. For example, users should be encouraged to go through the privacy policy terms before accept them and to act against the unjustifiable articles, which will be discussed in Section 4.1.

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 [92], Malhotra *et al.* [88], Tsai *et al.* [120]	2001, 2004, 2011	Pointing out the biggest fear for online shopping experiences	Surveys on Internet users	Lacking of deep analysis to build the privacy protection trust between the online shopping websites and the customers
Shiau and Luo [115], Bergström [15]	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.* [105]	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

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, 29]. Successful ridesharing platfoms, 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 estimated cost and assign a driver to the passenger. The payment is made by credit card associated with his/her account. In the end, both the passenger and the driver will rate each other.

Obviously, the mobile app tracks the users' location information as well as travel information. The driver also has the access to the rider's travel information such as riders' names, trip starting points and destinations. Under current privacy policies, riders have to share part of the private information in order to be serviced. 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 internal misuse of user data within the ridesharing companies. For instance, staffs in the ridesharing companies have the access to track the movements of customers. Taking Uber as an example, its privacy policy states that the Uber app collects and uses users' geo-location data for a variety of purposes, including internal business purposes. However, such purposes are not defined explicitly. As a matter of fact, most of the users are not aware of how their geo-location data being used. Additionally, Uber can also "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" [71] by Uber. Nevertheless, users do not know what information is necessary or appropriate.

Location privacy has been studied extensively due to the increasing popularity of location-based services such as mobile apps [9, 14, 16, 91, 114]. While location-aware applications track users' location or other data online, they generate huge amount of potentially sensitive data. The privacy of location data is about regulating access to the data. It is not necessary nor possible to forbid all access because the systems have to access the data in order to provide a better service. However, the access should be restricted to authorized persons and should never be exposed to others. In other words, the data and the access should be in control and only accessed with legal authorization [14].

Kido *et al.* [72] proposed an anonymous communication technique for location-based services to protect location privacy using adding noises to the location data. When a user sends an enquiry to the server, he sends his true 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 real location of the user; but the location based server (LBS) is able to find the difference through optimized algorithms with external information such as the road navigation service (RNS) data. The obvious shortage of Kido *et al.*'s work is that the real location is not completely concealed. There are still chances for the observer to identify the real location.

Yao *et al.* [136] provided an effective encryption service for location information of users with the clustering K-anonymity (CK) scheme. The CK scheme encrypt the user location information by a cloaked spatial temporal boundary (CSTB) involving 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 [101] extended Yao *et al.*'s work using a p-anti-conspiration privacy model to hide the exact location of users. They studied various techniques to provide location based services without knowing the exact location of the users. It is a big advancing step for the ridesharing companies to protect the user locations. An improvement work done by the same group of authors in [100] shows that the insufficiencies still exist in the aspect of protecting sensitive information.

Jagwani and Kaushik [65] introduced the concept and structure of zero knowledge proof (ZKP) to defend the location privacy. They explained the detailed construction process of the ZKP and discussed

the possible applications of ZKP in the location based service domain. Their method requires a third party middleware to act as a trusted agent.

Gao *et al.* [48] pointed out that the trajectory privacy, which contains the spatial-temporal information, must be added to location privacy protection scheme. In their study, they proposed a trajectory privacy-preserving framework to protect the trajectory privacy. A mixed-zone graph model is utilized to demonstrate the effectiveness of the proposed scenarios. The main shortage of the framework is that the exact location must be revealed to a third party middleware.

In recent years, online social networks or geosocial information started to be used in ridesharing services. The purpose is to recommend users to join their friends' cars instead of strangers'. Based on this motivation, Elbery *et al.* [42] 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 friends.

Ni *et al.* [97] suggested the users to hide their true identity by bringing an anonymous mutual authentication (AMA) protocol into the carpooling recommendation system. A real-time navigation system is proposed to conceal the drivers' privacy [96]. The important features of their applications include false information traceability, where the trusted third party authority can trace wrong information either from a user or a driver. The limitation of their work is that a trusted third party is still required.

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

The main reviewed papers are summarized in Table 5. We indicate that although there are multiple privacy concerns in the ridesharing services, such as the user queries and trajectory information, the location information protection is still the most emerging topic in this area [35].

3.3 Homesharing

Homesharing is a business model which connects hosts and travelers through an online marketplace platform and enables transactions without owning any rooms itself. It does not provide the rental services directly, instead it matches hosts who have extra rooms for renting and travelers who need a room for stay [47, 102]. One of the most famous homesharing platforms is Airbnb [66].

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

Franzetti [45] conducted a deep analysis on sharing economics and pointed out that the regulation of homesharing still had a large gap for improvement. In the current stage of sharing services, it is much safer for travelers to stay in a hotel rather than be involved in a homesharing service. There's no concrete suggestion of regulation improvement in the article.

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

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.* [72]	2005	Protecting location privacy using dummies	An anonymous communication technique	The real location is not completely concealed
Yao *et al.* [136]	2010	Encrypting the user location information	Clustering K-anonymity (CK) scheme	Decreasing location information resolution and degrading the QoS
Pan and Meng [101]	2013	Providing location based services without knowing the exact location	The p-anti-conspiration privacy model	lacking of 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.* [48]	2013	Protecting the trajectory privacy	A trajectory privacy-preserving framework	The exact location must be revealed to a third party middleware
Ni *et al.* [96, 97]	2016	Concealing both users and drivers' sensitive information	An anonymous mutual authentication (AMA) protocol	A trusted third party is required
Aïvodji *et al.* [3]	2016	Computing the mutual interested meeting point	Multimodal routing algorithms	A more complicated system involving multiple drivers and riders are left for future exploration

Ert *et al.* [43] designed an experiment using mixed-logit analysis to discuss the relationship of posting 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 raise the likelihood of the house to be booked. However, the relationship between the trust and privacy preservation is not discussed deeply.

On the other hand, the risks of being a host, including posting host's photo and identity information, in the homesharing practices are discussed by Hooshmand [60]. But the leakage of the hosts' privacy can be another issue in the homesharing practices. While it is unlikely to solve the regulation problems through a single method, it is quite possible to protect the privacy of both hosts and travelers through the joint efforts of hosts, travelers, platforms and governments. We list all reviewed works for security concerns of homesharing in Table 6.

3.4 Summary and Discussion

Collaborative consumption collects extra or redundant resources and distributes them to people who do not have accesses to them. In practice, users are subject to information leakage due to the exchange of data and improper use of user data by the internal staffs of the platforms. While it is difficult to provide

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

Reference	Year	Main objective	Proposed solution	Important insufficiency
Franzetti [45]	2015	Pointing out that the regulation of homesharing still had a large gap for improvement	A deep analysis on Airbnb service	lacking of concrete suggestion on regulation improvement
Kamal [68]	2016	Building trust in homesharing practices	Proposing additional security checks	not discussing the cost of additional security measurements
Ert *et al.* [43]	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
Hooshmand [60]	2015	Stating the risks of being a host	Possibilities of improving the homesharing regulation	Possibly leaking private information of the hosts

an absolute privacy-safe environment without sacrificing the service quality, it is possible to increase the protection levels of privacy through a joint effort of all participants, platforms and governments.

There are other methods available to protect privacies in the collaborative consumption practices. Milberg *et al.* [90] studied the relationships among nationality, cultural values, personal information privacy concerns, and information privacy regulation. The study shows that the lack of interpersonal trust among individuals in a society may result in desire for more government involvement to protect personal information privacy. Luo *et al.* [81] examined several mechanisms to increase customers' trust of e-commerce and decrease privacy concerns through building trust. Such mechanisms include characteristic-based, transaction process-based, and institution-based trust production. Nissenbaum [98] discussed privacy in the perspective of contextual integrity in technology, policy and social life.

4 SUMMARIZING EMERGING PRIVACY ISSUES FROM USER AND SERVICE PROVIDER PERSPECTIVES

The fast development of cyber technology facilitates the invention of novel sharing practices in the cyber-enabled world. While the traditional privacy problems are either solved or at least realized by the government and society, privacy issues in cyber-enabled sharing services are less realized and more emerging for security purposes. In all six branches of the taxonomy in Figure 1, there are always interactions between user, middleware and service provider. The privacy protection issues were always discussed from these three perspectives in the reviewed works.

In this section, we point out the most emerging issues in the current stage of cyberized sharing service development from three perspectives, i.e. user, middleware and service provider perspectives. We summarize that the most emerging issues are increasing the user privacy awareness from user perspective, protecting shared information from middleware perspective and enhancing privacy protection realization from the service provider perspectives. A list of all reviewed works are depicted in Figure 7.

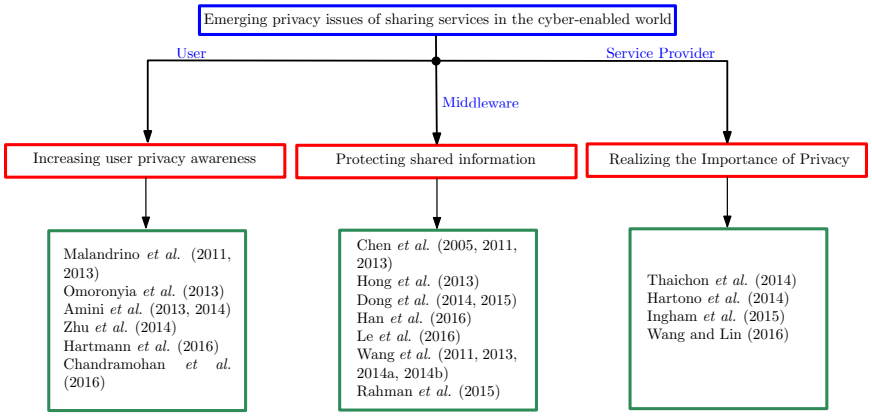

Fig. 7. The emerging privacy issues in the current stage of cyberized sharing service development from user and service provider perspectives.

4.1 From User Perspective: Increasing Privacy Awareness

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

For example, in the crowdsourcing marketplace, it is not sufficient to only protect 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) [119, 134]. According to the survey in U.S. Federal Trade Commission's consumer privacy report 2012 [36], more than 85% of the users were impatient to read the user agreements regarding privacy settings carefully. They were surprised that the mobile phone apps sent their approximate or precise location, phone's unique ID to the providers. Some apps even have the control of the camera flashlight and audio settings. Though privileges were authorized by users, the users did not know when or where they did the authorization, because they never read the articles about privacy settings. Some efforts have been made to solve the above problem.

Malandrino *et al.* [86, 87] implemented a privacy awareness software which is named as 'NoTrace'. The software provides services, such as automatic setting for protecting privacy, measurement of personal data revealed by service provider and awareness of privacy leakage to third-party websites. The graphical user interface of 'NoTrace' is shown in Figure 8, which displays clearly the privacy elements received by the service provider. However, they did not provide a deep analysis on which data elements are necessary for the service and which are not. The analysis provides useful hints for the users as well as the service provider to selectively share the private information.

Omoronyia *et al.* [99] developed an adaptive privacy framework to assist privacy disclosure decisions 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 benefits from privacy disclosure. The insufficiency of their work is lacking of systematical privacy requirements listing for a given set of service functions [89].

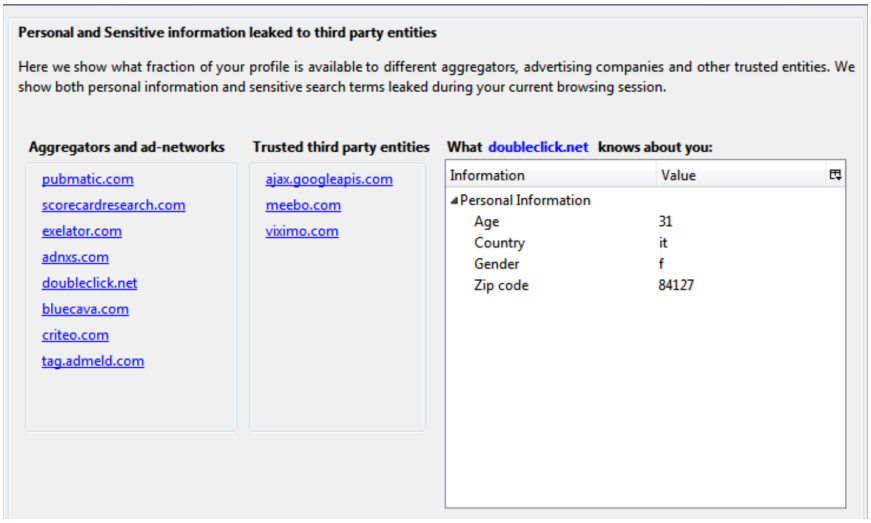

Fig. 8. The 'NoTrace' software graphic user interface, developed by Malandrino *et al.* [86, 87].

Amini *et al.* [4, 5] proposed a software called AppScanner to help users better understand the functionality of mobile applications. The software provides informative description of what mobile apps are really doing under a crowdsourcing environment. The transparency and detailed analysis of the mobile apps help users aware possible privacy leakage by using mobile apps for crowdsourcing. The AppScanner only categorizes the mobile apps behaviors as normal and abnormal. In fact, a detailed categorization according to the behaviors purposes, e.g. advertising and social networks, can be more helpful for the users to make the right choices [133].

Zhu *et al.* [141] 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 raises a recommendation to the user of whether to continue use the mobile app according to the app's popularity and user settings. The recommendation is made based on the modern portfolio theory. The main shortage of the recommendation system is that the security risks are only evaluated based on the permissions that the apps request.

Hartmann *et al.* [55] summarized six main threats of mobile apps for the users to aware potential privacy risks. The six threats include: insufficient control features, excessive data mining, data theft, surveillance, information leakage and social engineering. They also proposed eight recommendations for these privacy threats, which are: 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 developments. However, the immediate solutions of all conflicts are still lacking.

Chandramohan *et al.* [30] pointed out that cloud users are compelled to share their personal information with the service provider by accepting the user agreements. Only 5% to 10% of the users aware that their personal information might be misused. Chandramohan *et al.* described a complete scheme called Petri-net Privacy Preserving Framework (PPPF) to protect the user privacy on cloud. However, the practicability and real-time applicability of their algorithm need further discussion.

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.* [86, 87]	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.* [99]	2013	Assisting privacy disclosure decisions made by applications	An adaptive privacy framework	Lacking of 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.* [141]	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.* [55]	2016	Addressing threats of mobile apps and proposing solutions	Eight recommendations for six main threats	No immediate solution is provided
Chandramohan *et al.* [30]	2016	Protecting user privacy on cloud	Petri-net Privacy Preserving Framework	The practicability and real-time applicability of their algorithm need further discussion

In summary, all above mentioned works, which we list in Table 7, suggest that the privacy leakage in some level is unavoidable in order for the users to enjoy the sharing service. But technical effort can be valuable to help users realize the portion of information which is shared. The users can make their own decision on whether to use the particular sharing service according to their preference.

4.2 From Middleware Perspective: Protecting Shared Information

Although users may agree to share part of their personal Information in order to enjoy the sharing services, the shared information/data is still required to be protected from the third party middleware. Most third party middleware pieces use cyber technologies, such as cloud computing, to analyze the shared user data. The purpose of data analysis is for better service quality. However, privacy concerns influence users to provide spurious information. The second emerging privacy issue is to establish an effective protocol to protect the privacy in the data analysis process. In this section, we surveyed several state-of-art works for the protocol design of the data analysis system to protect the privacy.

Chen *et al.* [31, 33, 34] presented a random space encryption (RASP) approach to provide efficient and secure classifier using cloud computing technology with privacy preserved. The RASP approach provides service to transfer the analyzing data into an encrypted space with a two-stage encoding algorithm. In

their study, they also pointed out that updating the encrypted database is another challenge to their work.

Hong *et al.* [59] surveyed several existing privacy protection strategies under the distributed data sharing environment. They pointed out the privacy protection techniques can be applied to the database, queries or aggregation. Specifically, they focused on privacy preserving schemes on time series data processing for data mining.

Dong *et al.* [38, 39] suggested a privacy-preserving data security policy, by utilizing ciphertext policy attribute-based encryption (ABE) combined with identity-based encryption (IBE) techniques. The proposed framework allows the users to dynamically access their own personal data freely. Both ABE and IBE were used to minimize the key management overhead; however, the proposed method resulted in key escrow problems [110].

Following Dong *et al.*'s work, Han *et al.* [54] provided a promising solution for privacy-preserved data outsourcing under cloud environment. They proposed an ABE based privacy protected data access control scheme on the cloud which solves both the key-escrow and revocation problems. The time complexity of both encryption and decryption processed in the proposed method requires further improvement.

Le *et al.* [75] 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 rule regulations might not be applicable under certain conditions.

Wang *et al.* [80, 130–132] proposed a hierarchical attribute-based encryption (HABE) scheme to keep the shared data confidential against untrusted cloud service providers. The general structure of the HABE scheme is depicted in Figure 9. The trusted third party (TTP) is responsible to generate and distribute of keys to the domain masters. The domain master generates keys to a specific group of users in the next sub-level. Specifically, 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 addition, they also proposed an scalable revocation scheme for users to access their own personal data. The proposed scheme lacked of user revocation and was only applicable under the situation that all attributes were administered by the same domain authority.

Rahman *et al.* [107] reviewed 139 works from 2009 to 2014 about information security in cloud computing. Specifically, they focused on the incident handling strategy (IHS) which is an important tool for protection data in a shared cloud service system. It is pointed out that although the IHS is straightforward in personal PC, it becomes complicated while the cloud computing allows multiple computers to access the same data on the same hard-disk. They proposed an information protection model for the shared data on cloud combining IHS and digital forensics principles.

In summary, a list of surveyed works can be found in Table 8. We believe that establishing an effective protocol in the middleware is beneficial for both users and service providers. Although the data analysis is necessary for service quality improvement, it is essential to be processed under well-regulated schemes or systems.

4.3 From Service Provider Perspective: Realizing the Importance of Privacy

As the last but important participant, the service providers have to learn the importance of protecting user privacy. Numerous studies have shown that the privacy protection/security quality is an important component of the service quality in overall, and therefore influences the final profit of the company [27, 118, 139]. More specifically, the enhancement of privacy protection quality from the service provider potentially attracts more customers to pay for the service [26].

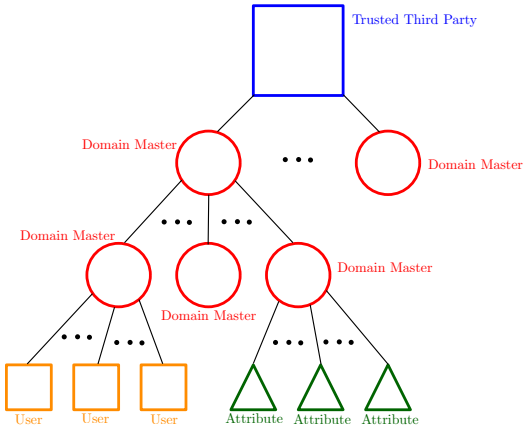

Fig. 9. The hierarchical attribute-based encryption (HABE) scheme proposed by Wang *et al.* [80, 130–132].

Thaichon *et al.* [118] surveyed the relationship between various aspects of service quality and the perceived value from customers. They have concluded the four most important service quality dimension influencing the final profit of the company, which are: network quality, customer service quality, information quality and security/privacy protection quality. The main limitation of their study is that the survey is only conducted in the context of a single country (i.e. Thailand).

Hartono *et al.* [56] further identified the most important dimensions of perceived security for online purchases as confidentiality, integrity, availability and non-repudiation. They validate that these four aspects significantly impact the customer's willingness on participating e-commerce services by using a second-order structural model on perceived security. In their experimental part, only responses from Korea are used, which can potentially reduce the generalization of the study results.

Ingham *et al.* [64] examined the internal relationship between trust, perceived risks and customers' acceptance in the e-shopping practices. The technology acceptance model (TAM) nomological network is deeply discussed to measure the values in different dimension. The testing results is analyzed by meta-analytical path analysis. It was a comprehensive survey paper looking for potential ways to promote e-commerce for better sales. However, the substantial techniques of enhancing the trusts gained from the customers are missing.

Wang and Lin [129] established a research conceptual framework to study the internal linking of service quality and intention of continuous usage of location based services (LBS) (Figure 10). By a survey size of 1399 questionnaires, Wang and Lin concluded that the information quality, system quality, and service quality have positive influence on perceived trust which is negatively related to privacy trust and positively related to continuous usage of LBS. The culture concern existed in their work since the survey was only conducted in Taiwan.

The list of all surveyed works from the service providers' perspective is shown in Table 9. In summary, we would like to point out that the privacy protection level is an essential part in service quality measurement and will significantly impact on the customer willingness of participation, trust and net profit. As a result, it is important to raise the privacy issues to the service providers and improve their commercial strategies by providing more secure servicing environment.

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.* [31, 33, 34]	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.* [59]	2013	Preserving privacy under distributed environment	Surveying existing privacy protection strategies	Mainly focusing on time-series data mining
Dong *et al.* [38, 39]	2014, 2015	Suggesting a privacy-preserving data security policy	A series of encryption techniques	Resulting in key escrow problems
Han *et al.* [54]	2016	privacy-preserved data outsourcing under cloud environment	ABE based privacy protected data access control scheme	Requiring efficiency improvements
Le *et al.* [75]	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.* [80, 130–132]	2011, 2013, 2014	Keeping the shared data confidential against untrusted cloud service providers	The hierarchical attribute-based encryption (HABE) scheme	lacking of user revocation and was restricted by the same domain condition
Rahman *et al.* [107]	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

5 CONCLUSION

In this paper, we studied the privacy issues in sharing service practices in the current stage of cyber-enabled world. We divided the sharing services into two categories, namely crowdsourcing and collaborative consumption. Both categories are further divided into three branches. The in total six branches comprehensively covers the sharing service practices in the cyber-enabled digital world. Most surveyed works, analyses, results and solutions from the recent five years, i.e. from 2011 to 2016. Figure 11 depicts the time-line statistical distribution of all listed surveyed works from Table 1 to 9.

The crowdsourcing is further divided into three branches: Internet crowdsourcing marketplace, crowdfunding and crowdtesting. In Internet crowdsourcing marketplace practices, we tackle the privacy protection problem for the requesters. Two approaches are surveyed, which are the coding theory and the instance clipping protocol. Various solutions to protect the requester's privacy were proposed extending

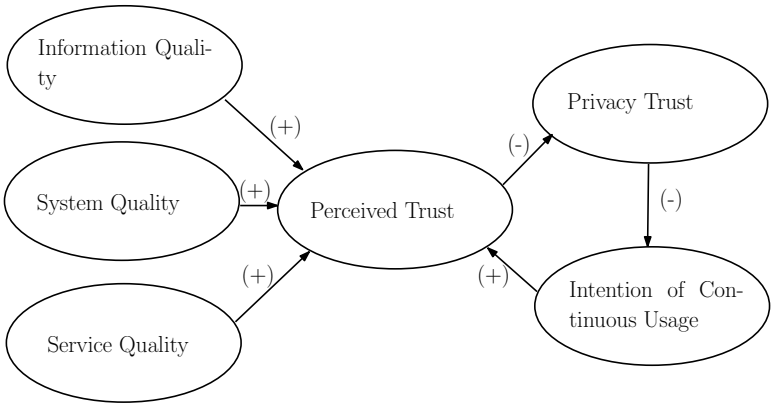

Fig. 10. The research conceptual framework proposed by Wang and Lin studies on the relationship between various elements on service quality and the intention of continuous usage of location based services [129].

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.* [118]	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.* [56]	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.* [64]	2015	Examining the internal relationship between trust, perceived risks and customers' acceptance	The technology acceptance model (TAM) nomological network	Lacking of ways to gain the customers' trusts
Wang and Lin [129]	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

the two approaches. In crowdfunding and crowdtesting practices, fundraiser's credential and tester's reliability are identified as the emerging issues for the two two types of sharing services respectively.

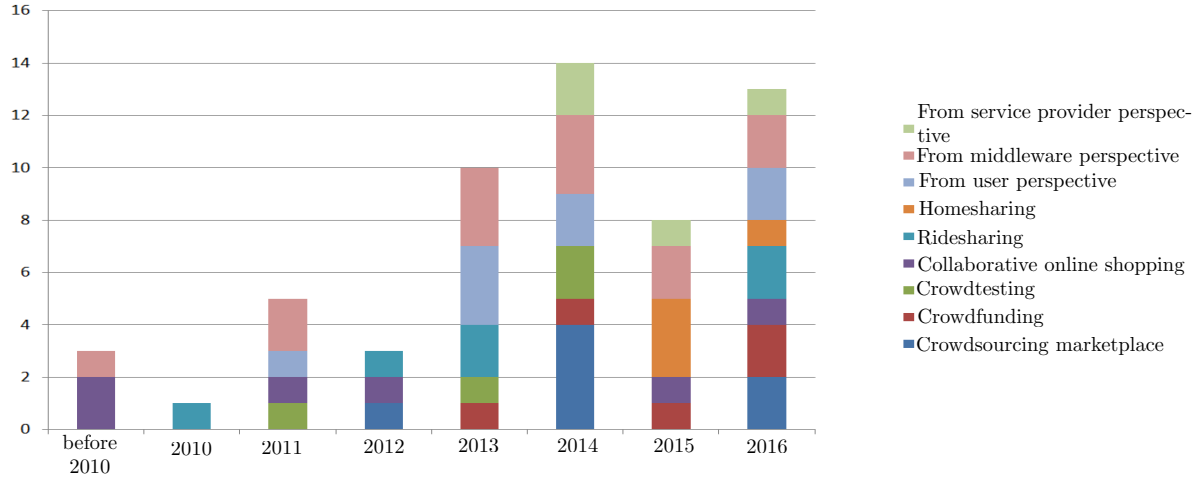

Fig. 11. The time-line statistics of all listed surveyed works from Table 1 to 9.

In collaborative consumption, the three sub-categories are: collaborative online shopping, ridesharing and homesharing. The collaborative online shopping, as a new generation of online shopping experience, is the most representative collaborative consumption form in the sharing practices. The trusts between users, security systems, shopping websites and service providers are identified as the major factors that stop people participating the collaborative online shopping practices. We reported several survey results to verify the major privacy concern with numerous possible solutions. For rideshaing and homesharing practices, the location privacy and the homesharing risks are the two major privacy concerns for the two types of sharing services respectively.

Last, we summarize the privacy concerns in the cyber-enabled sharing world from three perspectives. From the user perspective, users start to realize that they have to sacrifice certain degree of personal information in order to enjoy the sharing services. Therefore, the most emerging issue is to raise the privacy awareness of the users. From the middleware perspective, it is necessary for the third party middleware to analyze the user shared data to improve the service quality. The emerging issue from the middleware perspective is to develop an effective protocol to preserve the privacy in the data analysis process. From the service provider perspective, it is important to realize that the privacy concern is part of the service quality which potentially impacts the user perceived security, trust and the final profit.

Future works of this study include developing more readable user agreement to completely settle the user awareness of privacy control, and designing mechanisms on regulating service provider's behavior from government perspectives.

Conflict of Interests

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

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China, under grant 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] Stephanos Androutsellis-Theotokis. 2002. A survey of peer-to-peer file sharing technologies. (2002).

[8] Nic Baddour. 2011. Indiegogo Insight: Pitch Videos Power Contributions-Increasing Them 114%. (2011).

[9] 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.

[10] 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.

[11] Russell Belk. 2014. You are what you can access: Sharing and collaborative consumption online. *Journal of Business Research* 67, 8 (2014), 1595–1600.

[12] 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.

[13] Paul Belleflamme, Thomas Lambert, and Armin Schwienbacher. 2014. Crowdfunding: Tapping the right crowd. *Journal of Business Venturing* 29, 5 (2014), 585–609.

[14] Alastair R Beresford and Frank Stajano. 2003. Location privacy in pervasive computing. *IEEE Pervasive computing* 1 (2003), 46–55.

[15] 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.

[16] Claudio Bettini, X Sean Wang, and Sushil Jajodia. 2005. Protecting privacy against location-based personal identification. In *Secure data management*. Springer, 185–199.

[17] Rachel Botsman and Roo Rogers. 2010. Beyond zipcar: Collaborative consumption. *Harvard Business Review* 88, 10 (2010), 30.

[18] Rachel Botsman and Roo Rogers. 2010. Whats mine is yours. *The Rise of Collaborative Consumption* (2010).

[19] Rachel Botsman and Roo Rogers. 2010. What's mine is yours: The Rise of Collaborative Consumption. (2010).

[20] Rachel Botsman and Roo Rogers. 2011. *What's mine is yours: how collaborative consumption is changing the way we live*. Collins London.

[21] 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.

[22] C Steven Bradford. 2012. The New Federal Crowdfunding Exemption: Promise Unfulfilled. *Securities Regulation Law Journal* 40, 3 (2012).

[23] 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)*.

[24] 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)*.

[25] 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.

[26] 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.

[27] 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.

[28] 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.
[29] Nelson D Chan and Susan A Shaheen. 2012. Ridesharing in north america: Past, present, and future. *Transport Reviews* 32, 1 (2012), 93–112.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] Keke Chen and Ling Liu. 2005. Privacy preserving data classification with rotation perturbation. In *Data Mining, Fifth IEEE International Conference on*. IEEE, 4–pp.
[35] Delphine Christin. 2016. Privacy in mobile participatory sensing: Current trends and future challenges. *Journal of Systems and Software* 116 (2016), 57–68.
[36] Federal Trade Commission and others. 2012. Protecting consumer privacy in an era of rapid change. *FTC Report, Washington, DC* (2012).
[37] 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.
[38] 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.
[39] 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.
[40] AJ du Croix. 1985. Data sharing and access protection in Business System 12. *Computers & Security* 4, 4 (1985), 317–323.
[41] Khaled El Emam, Fida Kamal Dankar, Romeo Issa, Elizabeth Jonker, Daniel Amyot, Elise Cogo, Jean-Pierre Corriveau, Mark Walker, Sadrul Chowdhury, Regis Vaillancourt, and others. 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.
[42] 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.
[43] 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).
[44] M Feeney. 2015. Is ridesharing safe? Cato Policy Analysis, 27 January, no. 767. (2015).
[45] Andres Franzetti. 2015. Risks of the sharing economy. *Risk Management* 62, 3 (2015), 10–12.
[46] 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.
[47] Vishal Gaikar. 2013. First eBay, Now AirBnB: The Rise of Peer to Peer Marketplaces. (2013).
[48] 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.
[49] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. 1998. Protecting data privacy in private information retrieval schemes. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*. ACM, 151–160.
[50] Eric Gilbert, Kathi Evans, Troy Clark, and Karl Beck. 2001. De-identification and linkage of data records. (Aug. 15 2001).
[51] MaryAnne M Gobble. 2015. Regulating Innovation in the New Economy. *Research-Technology Management* 58, 2 (2015), 62.
[52] 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).
[53] Juho Hamari, Mimmi Sjöklint, and Antti Ukkonen. 2015. The sharing economy: Why people participate in collaborative consumption. *Available at SSRN 2271971* (2015).
[54] Ke Han, Qingbo Li, and Zhongliang Deng. 2016. Security and efficiency data sharing scheme for cloud storage. *Chaos, Solitons & Fractals* 86 (2016), 107–116.

[55] Heinrich Hartmann, Tim Wambach, Maximilian Meffert, and Rüdiger Grimm. 2016. A privacy aware mobile sensor application. (2016).
[56] 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.
[57] Johannes Heurix, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz. 2015. A taxonomy for privacy enhancing technologies. *Computers & Security* 53 (2015), 1–17.
[58] Matthias Hirth, Sven Scheuring, Tobias Hoßfeld, Christian Schwartz, and Phuoc Tran-Gia. 2014. Predicting result quality in crowdsourcing using application layer monitoring. In *Communications and Electronics (ICCE), 2014 IEEE Fifth International Conference on*. IEEE, 510–515.
[59] 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.
[60] Mark Hooshmand. 2015. The risks of being a host in the sharing-economy. (2015).
[61] Tobias Hoßfeld, Christian Keimel, Matthias Hirth, Bruno Gardlo, Julian Habigt, Klaus Diepold, and Phuoc Tran-Gia. 2013. CrowdTesting: a novel methodology for subjective user studies and QoE evaluation. *University of Würzburg, Tech. Rep* 486 (2013).
[62] Tobias Hoßfeld, Christian Keimel, Matthias Hirth, Bruno Gardlo, Julian Habigt, Klaus Diepold, and Phuoc Tran-Gia. 2014. Best practices for QoE crowdtesting: QoE assessment with crowdsourcing. *IEEE Transactions on Multimedia* 16, 2 (2014), 541–558.
[63] Jeff Howe. 2006. The rise of crowdsourcing. *Wired magazine* 14, 6 (2006), 1–4.
[64] 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.
[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] 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).
[70] Orin S Kerr. 2003. Internet surveillance law after the USA Patriot Act: The big brother that isn't. *Available at SSRN 317501* (2003).
[71] Sabreena Khalid. 2014. Privacy Concerns in the Sharing Economy: The case of Uber. (2014).
[72] 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.
[73] 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.
[74] 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).
[75] 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.
[76] 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.
[77] Yan Li, Yingjiu Li, Qiang Yan, and Robert H Deng. 2015. Privacy leakage analysis in online social networks. *Computers & Security* 49 (2015), 239–254.
[78] David A Light. 2013. Sure, you can trust us. *MIT Sloan Management Review. v43 i1* 17 (2013).
[79] 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.
[80] 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.
[81] 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.

[82] 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.
[83] 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)*.
[84] 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.
[85] Alison Macrina. 2015. The Tor browser and intellectual freedom in the digital age. *Reference & User Services Quarterly* 54, 4 (2015), 17.
[86] 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.
[87] 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.
[88] 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.
[89] Rene Meis and Maritta Heisel. 2016. Computer-aided identification and validation of privacy requirements. *Information* 7, 2 (2016), 28.
[90] 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.
[91] 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.
[92] 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.
[93] Ricky KP Mok, Weichao Li, and Rocky KC Chang. 2015. Detecting low-quality crowdtesting workers. In *2015 IEEE 23rd International Symposium on Quality of Service (IWQoS)*. IEEE, 201–206.
[94] Ethan Mollick. 2014. The dynamics of crowdfunding: An exploratory study. *Journal of Business Venturing* 29, 1 (2014), 1–16.
[95] Robert Morgan. 2015. CYBER LIFE. (2015).
[96] 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.
[97] 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.
[98] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
[99] 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.
[100] 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.
[101] Xiao Pan and Xiaofeng Meng. 2013. Preserving location privacy without exact locations in mobile services. *Frontiers of Computer Science* 7, 3 (2013), 317–340.
[102] 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.
[103] 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.
[104] Yves Poullet. 2006. EU data protection policy. The Directive 95/46/EC: Ten years after. *Computer Law & Security Review* 22, 3 (2006), 206–217.
[105] 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.
[106] pybossa. 2015. PYBOSSA. (2015). pybossa.com.

[107] 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.
[108] 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.
[109] Jeffrey M Rzeszotarski and Aniket Kittur. 2011. Instrumenting the crowd: using implicit behavioral measures to predict task performance. In *Proceedings of the 24th annual ACM symposium on User interface software and technology*. ACM, 13–22.
[110] 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.
[111] Pierangela Samarati and Latanya Sweeney. 1998. Generalizing data to provide anonymity when disclosing information. In *PODS*, Vol. 98. 188.
[112] Juliet Schor. 2014. Debating the sharing economy. *essay published by the Great Transition Initiative, Tellus Institute, available at http://www. greattransition. org* (2014).
[113] Paul M Schwartz. 2004. Property, privacy, and personal data. *Harvard Law Review* (2004), 2056–2128.
[114] 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.
[115] 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.
[116] B Sullivan. 2002. Ebay Privacy Policy Draws FireAgain. *Computerworld, March* 20 (2002).
[117] Latanya Sweeney. 2002. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, 05 (2002), 557–570.
[118] 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.
[119] 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.
[120] 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.
[121] 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.
[122] Debra A Valentine. 2000. Privacy on the Internet: The evolving legal landscape. *Santa Clara Computer & High Tech. LJ* 16 (2000), 401.
[123] Lav R Varshney. 2012. Privacy and reliability in crowdsourcing service delivery. In *2012 Annual SRII Global Conference*. IEEE, 55–60.
[124] 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.
[125] 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.
[126] 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.
[127] Kim-Phuong L Vu and Robert W Proctor. 2016. User Privacy Concerns for E-Commerce. (2016).
[128] Maja Vuković. 2009. Crowdsourcing for enterprises. In *Services-I, 2009 World Conference on*. IEEE, 686–692.
[129] 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.
[130] 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.
[131] 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.
[132] 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.
[133] 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.

[134] Yang Wang, Yun Huang, and Claudia Louis. 2013. Respecting user privacy in mobile crowdsourcing. *SCIENCE* 2, 2 (2013), pp–50.
[135] Adrian Wright. 2001. Controlling risks of E-commerce Content. *Computers & Security* 20, 2 (2001), 147–154.
[136] 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.
[137] Hu Ying. 2015. Regulation of Equity Crowdfunding in Singapore. *Sing. J. Legal Stud.* (2015), 46.
[138] 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).
[139] 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.
[140] 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.
[141] 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.