Privacy in Crowdsourcing: A Systematic Review

Abdulwhab Alkharashi
Karen RenaudAuthor

This is the Author Accepted Manuscript of a conference paper published in Information Security: 21st International Conference, ISC 2018, Guilford, UK, September 9-12, 2018, Proceedings. Lecture Notes in Computer Science, vol 11060

The final publication is available at Springer via https://doi.org/10.1007/978-3-319-99136-8_21

Privacy in Crowdsourcing: A Systematic Review

Abdulwhab Alkharashi[1] and Karen Renaud[2,1]

[1] University of Glasgow, Glasgow, Scotland
[2] Abertay University, Dundee, Scotland
a.alkharashi.1@research.gla.ac.uk ; k.renaud@abertay.ac.uk

Abstract. The advent of crowdsourcing has brought with it multiple privacy challenges. For example, essential monitoring activities, while necessary and unavoidable, also potentially compromise contributor privacy. We conducted an extensive literature review of the research related to the privacy aspects of crowdsourcing. Our investigation revealed interesting gender differences and also differences in terms of individual perceptions. We conclude by suggesting a number of future research directions.

Keywords: privacy principles, privacy aspects, crowdsourcing

1 Introduction

Crowdsourcing concatenates the words 'crowd' and 'outsourcing' to reflect platforms that facilitate the recruiting of "crowds" to undertake tasks. The crowdsourcing approach has the potential to provide organizations with access to new ideas and solutions, to engender sustained consumer engagement and opportunities. It constitutes a step change in the way many people work, hire, and market labour [13, 42].

Crowdsourced labour is not always remunerated. In particular, Wikipedia is a widely known and used crowdsourcing platform where members donate their time to contribute to a publicly-available online encyclopedia. The outcome is the most inclusive encyclopedia in the world [14] that ranks as the fifth [69] most-viewed website worldwide.

The principle of crowdsourcing is that many heads are better than one. By recruiting a large crowd, it is possible to gather ideas, benefit from a wide variety of skills, and encourage participation. The quality of content and idea generation will be superior to anything produced by a solo person or small team [75].

Crowdsourcing, in addition to its positive aspects, also renders its users vulnerable to significant privacy risks. In this paper, we use previously-proposed privacy dimensions to evaluate the effectiveness of high-level guidance for enhancing privacy [27]. These include privacy categories [58, 60], privacy principles [32, 36, 77], privacy concerns [16] and privacy enhancements [77].

The contribution of this paper is to provide an overview of existing research into crowdsourcing-related privacy concerns. Our review revealed a gender difference in terms of crowdsourcing labourers and allows us to suggest possible future research directions.

2 Privacy

Solove [70, p. 1] defines privacy as *"a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations"*.

This definition informs our discussion of privacy challenges related to crowdsourcing. Computational systems have often not managed the enormous amount of data gathered by all these systems in a secure or confidential fashion. This could result in personal data being leaked and/or compromised [1]. Most of all, personal privacy could be sacrificed, and privacy, once lost, can never be regained.

In this section we outline the dimensions that informed our investigation. We will consider privacy from four distinct perspectives, and report on the interactions of these in published literature. The orthogonal dimensions are:

1. three basic **layers** of privacy derived from Patil & Kobsa [60]: *social, technical* and *legal*.
2. five privacy **principles** which are typically reflected in privacy legislation and regulations [32, 36, 77].
3. five privacy **concerns** experienced by people who give their personal data to others [16],
4. five privacy **enhancement** techniques that are typically applied by those who collect personal data in order to address specific individual concerns of the data owners [77].

These dimensions (depicted in Figure 1) provide the structure we used to inform our investigation.

(1) Privacy Layers

An extended view of a *layered framework* [58] was adapted from Patil & Kobsa [60] to allow us to analyze privacy risks from both user and service-provider perspectives.

Normative/Legal: this layer emphasizes laws and policies that protect the individual from the privacy-invasive practices engaged in by corporations, governments, and other individuals.

Technical: this layer describes measures put in place to protect personal data and to allow information owners to control access to their own information.

Social: this layer concerns the management of the boundary between people's private and public lives. Any information people divulge happens with an understanding of the context within which it is shared, and privacy is lost when the information is shared outwith that context.

We used these layers to identify the research gaps between privacy layers from legal, social and technical perspectives to identify the factors that shape privacy behaviours among online communities.

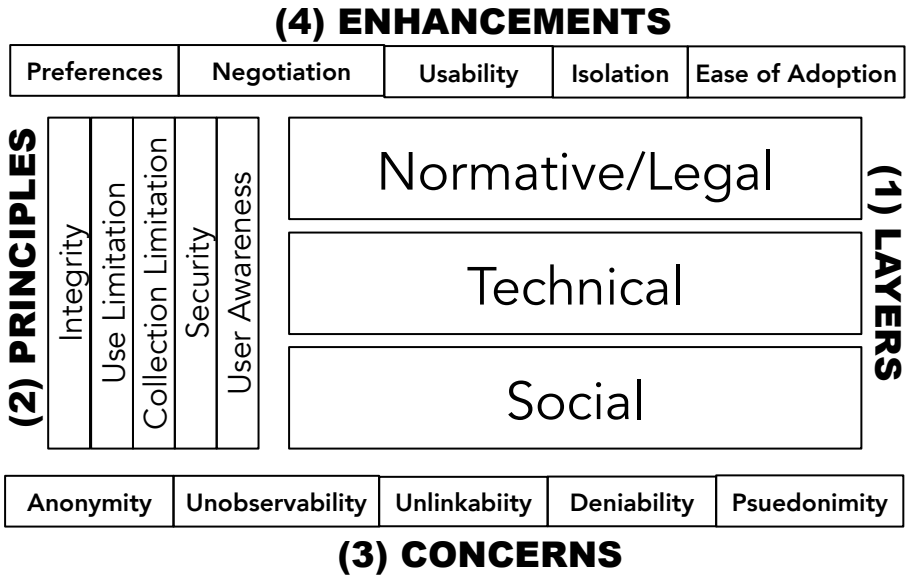

Fig. 1. Privacy Dimensions

(2) Privacy Principles

Privacy legislation and regulations typically instantiate fundamental privacy *principles*. We performed our analysis using a core set of privacy principles that are frequently addressed in privacy laws and regulations. The principles are briefly described below [77]:

User awareness. This indicates the level of clarity and knowledge of privacy when collecting or providing data [36].

Security. This concerns the reasonable security safeguards used to protect personal information and defend it against risks such as loss or unauthorized access, destruction, use, modification or disclosure of data [32].

Collection limitation. This concerns the limitations imposed onto the collection of personal data and the fact that any such data should be obtained by lawful and fair means [32].

Use limitation. This addresses the fact that personal data should not be disclosed, made available or otherwise used for purposes other than those specified during collection [32].

Integrity. This addresses the need for collected personal data to be sufficiently accurate and up-to-date to support the intended purposes. A data controller should ensure that all corrections are propagated in a timely manner to all parties that have received or supplied any inaccurate data that is identified [36].

(3) Privacy Concerns

Privacy *concerns* apply to an individual's particular views of justice within the context of privacy. People mostly have idiosyncratic views and interpretations of what data it is fair to collect, and how they rank their personal information from least to most sensitive. Campbell [16] suggests the following list of concepts that encapsulate people's concerns.

Anonymity. Ability to hide identity completely.

Pseudonymity. Appearances suggest identity hiding, but in reality the person can be identified.

Unobservability. Ability to use a system or websiye without all such accesses being logged.

Unlinkability. Ability for separate accesses not to be connected to each other by a data controller.

Deniability. Ability for users to deny some of their characteristics or actions, with the understanding that the system will not provide proof to refute such claims.

(4) Privacy Enhancement

A number of techniques are recommended for privacy *enhancement* [77].

User preference. A data controller should specify a service's privacy practices in line with each individual user's preferences.

Negotiation. Systems will facilitate a negotiation between a user and a website in terms of privacy standards.

Ease of adoption. This principle relates to the readiness of organizations to adopt a particular privacy protection, irrespective of the need for multiple infrastructures or technologies.

Usability. This principle relates to the ease with which users can convey their privacy decisions to the system.

Isolation. This principle relates to users being able to deny some of their characteristics or actions, and the understanding that others will not verify the veracity of their claims.

3 Systematic Review

In this section, we introduce a reproducible model of the systematic literature review process we conducted [37, 86]. The process, as shown in Figure 3, describes main stages of the review process: (1) selection, (2) specification and (3) summarizing.

Selection. in this process, we consider two important factors during selection. Firstly, we choose a particular key terms related to the research scope including: "crowdsourcing privacy", "crowd sourcing privacy"; or "crowdsourcing privacy" added with "social behavior", "user awareness", "security attacks", "concerns", "data protection", "trust", "anonymity", "integrity", "collection".

Secondly, we use multiple well-known digital library databases to collect all resources from: Web of Science, Directory of Open Access Journals, Microsoft Academic, Google Scholar, ProQuest, Research Gate, science Direct, IEEE Xplore Digital Library, arXiv (Cornell library) and Wiley.

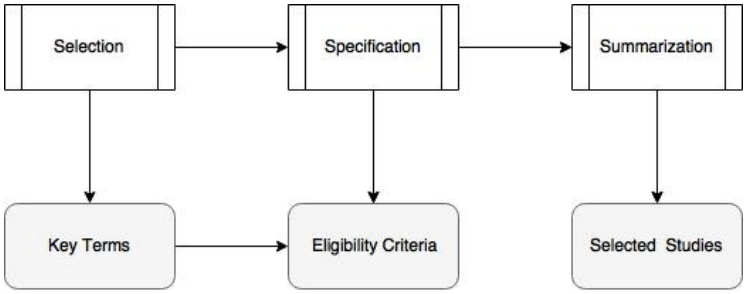

Fig. 2. Systematic Review Process

Specification. to manage our search results from a database source, we apply two simple rules of validation: date of publication and relevance of study. We only use papers that we can access online. We restricted our search to papers published from 2013 to 2017. Papers also should have enough information and must not be out of the research domain.

Summarizing: after we had filtered the papers, we recorded each paper's reference in our summary tables, finalized our full review of findings and discussed potential research directions.

4 Findings

Our search results on the online database delivered a total of 635 original research papers. We retained roughly 30% (212 papers): those that specifically discussed privacy in crowdsourcing.

Approaches Proposed by Researchers

We selected publications within four major approaches of research that correspond to crowdsourcing and privacy domains. These approaches are framework, algorithm, model and survey. Figure 3 shows that the number of published papers which presented model of privacy in crowdsourcing is research work (55%), algorithm (6%), survey (5%) and framework (34%). This also indicates that there is a research activity mostly in modeling and framework of privacy in crowdsourcing.

Privacy Principles

The papers were examined in terms of the privacy layers, principles, concerns and enhancements, as detailed in Section 2 as shown in Tables 1-3.

5 Discussion and Limitations

Two poorly researched areas were identified during the review: (1) Gender and Privacy, and (2) Individual Privacy Perceptions. We were not specifically looking for the first but it emerged during the analysis and we considered it worth reporting.

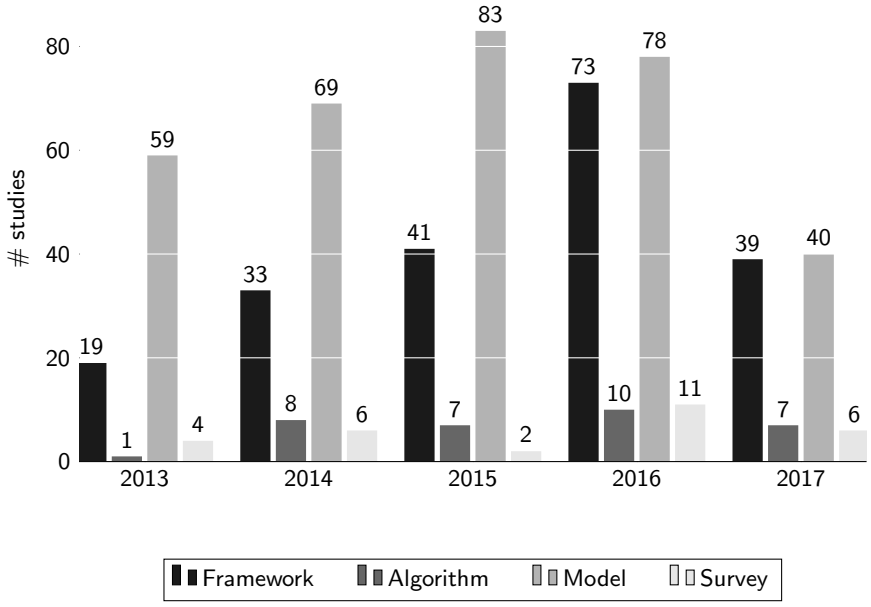

Fig. 3. The number of crowdsourcing privacy publications by research approach.

	User Awareness	Security	Collection limitation	Use limitation	Integrity
Privacy attitudes	[54, 59]	[56, 71]	[17]	[15, 17, 26]	•
Trust & evaluation	[82]	[63]	•	•	[28]
Intelligent applications	[7]	[2, 25]	•	•	[85]
Protection measures	[17, 73]	[35]	[22]	•	•
Authentication methods	[8]	[64]	•	•	[49]

Table 1. Summary of references dealing with Privacy Principles in crowdsourcing.

	Anonymity	Pseudonymity	Unobservability	Unlinkability	Deniability
Privacy attitudes	[47, 50, 76]	[34]	[34]	[34]	[34]
Trust & evaluation	[43, 63]	[72]	•	[78]	•
Intelligent applications	[23, 38]	•	[40]	•	•
Protection measures	[37]	•	•	•	•
Authentication methods	[10, 61]	•	[65]	•	•

Table 2. Summary of references related to Privacy Concerns in crowdsourcing.

	User preference	Negotiation	Ease of Adoption	Usability	Isolation
Privacy attitudes	[74]	[31]	•	[44]	[55]
Trust & evaluation	•	[57]	•	[57]	•
Intelligent applications	•	[41]	•	[20, 66]	[23]
Protection measures	•	•	•	[30]	•
Authentication methods	[4]	[79]	[12, 24]	[12]	[29]

Table 3. Summary of references relating to Privacy Enhancements in crowdsourcing.

Gender & Privacy:
Many studies report a gender gap in online knowledge sharing e.g. Wikipedia [6, 33, 52]. Researchers have shown that females are more concerned about online privacy than males [68] and it is just possible that privacy concerns are discouraging females from contributing. It would be interesting to test social psychology theory models in order gain a deeper understand of why this gap really exists and to gain insights into gender-specific privacy behaviours in this context. The main areas of gender gap revealed by reviewed literature are as follows:

Contribution. One study [51] shows that females contributed less to crowdsourced platforms during 2009. Only 16.1% of the 38,497 editors who started editing on Wikipedia were female. The study examined multiple social behaviour-related hypotheses by conducting statistical experiments when extracting Wiki page data. Another study reported that both males and females made the same number of revisions, and the most active female Wikipedians make more revisions than most active male Wikipedians.

Vandalism and trolling. Both acts have similar ultimate goals in the context of online discussion communities. However, these terms are used interchangeably in the research literature. Research around vandalism or trolling behaviour has tended to be essentially qualitative, commonly involving deep case-study analyses of a small number of manually-detected activities. These analyses include the different types of trolling that have been carried out [39], the motivations behind doing so [67] and the different approaches in terms of responding to trolls [9, 19]. Another study reports on the evolution of users' anti-social behaviours from initial joining to final banishment [18].

Measurement. The most common approach used by researchers when trying to understand behaviour is to use a measurement tool. One study [5] examines how contributor motivations affect the type of contributions made to Wikipedia by presenting a retention rate to measure the reliability of an article written by both registered and anonymous users. Another study has presented a machine learning approach to detect vandalism edits on Wikipedia by using a logistic regression model [62].

This particular finding suggests that the gender gap is an area that would benefit from further investigation, with a particular emphasis on gender-specific privacy-preserving behaviour in crowdsourcing.

Individual Privacy Perceptions:
Understanding privacy-based perceptions can be difficult. Most studies [45, 46, 48] suggest that crowd workers have similar amounts of personal information online. Yet different cultures have differing perspectives with respect to online anonymity and privacy [11]. The impact of culture and gender on privacy in crowdsourcing environments is a rich avenue for future investigation.

Research Limitations:
Although there is a huge intersect between the Internet of Things and crowdsourcing,

we restricted our review analysis to papers that applied privacy principles to the crowdsourcing context. We also included papers dealing with ubiquitous computing since these were also relevant. We restricted the date range to those published after 2014 to focus only on the most recent research. In a quickly-changing and developing research are, such as this one, research ages very quickly and old research is often no longer relevant in reflecting extant *status quo* research.

6 Related Research

Extensive research has been carried out related to privacy protection in ubiquitous computing [3, 53, 80]. One study [3] presents a mechanism to detect when users access private data. The idea is to provide a crowdsourced privacy recommendation engine on mobile applications to allow users to evaluate their privacy dimensions. There is an undeniable link between security and privacy and a number of research projects were conducted to reveal crowdsource-related security threats [81]. These systems are mostly useful for tracking and analysing the usage of sensitive data.

In public safety, crowdsourcing was used to study the information security factors when data is being collected from citizens that participate in crowdsourcing smart city project. [22]. In particular, it allows citizens to report unusual public-safety events by using mobile phone sensing applications to detect the location of crowdsourcing participants [21].

Several survey papers were presented in the context of crowdsourcing systems in general to describe the categories and characteristics of crowdsourcing applications [84], and to judge a crowdsourcing system to introduce solutions to address the challenges of crowdsourcing systems [83].

This systematic review revealed some interesting areas for future research in crowdsourcing privacy. Both privacy principles, concerns and enhancements have been addressed, yet the idea of combining these to study the gaps in crowdsourcing privacy research is a new one.

7 Conclusion

Although crowdsourcing platforms seem to grow so quickly in terms of both users and data, it is evident that privacy gaps still exist and are poorly covered in the research literature. Having reviewed the latest research on privacy in crowdsourcing, we plan to proceed to study editing behaviour in crowdsourcing next.

References

1. M Ackerman, T Darrell, and D J Weitzner. Privacy in context. *Human–Computer Interaction*, 16(2-4):167–176, 2001.
2. A Adamkó and L Kollár. A system model and applications for intelligent campuses. In *18th International Conference on Intelligent Engineering Systems (INES)*, pages 193–198. IEEE, 2014.

3. Y Agarwal and M Hall. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services*, pages 97–110. ACM, 2013.
4. F Alt, N Memarovic, M Greis, and N Henze. UniDisplay — A research prototype to investigate expectations towards public display applications. In *IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops),*, pages 519–524. IEEE, 2014.
5. D Anthony, S W Smith, and T Williamson. Reputation and reliability in collective goods the case of the online encyclopedia wikipedia. *Rationality and Society*, 21(3):283–306, 2009.
6. J Antin, R Yee, C Cheshire, and O Nov. Gender differences in Wikipedia editing. In *Proceedings of the 7th international symposium on Wikis and open collaboration*, pages 11–14. ACM, 2011.
7. M S Ashraf, S Saha, and S Shatabda. A Participatory Sensing Framework for Environment Pollution Monitoring and Management, 2017. arXiv preprint arXiv:1701.06429.
8. H Assal, S Hurtado, A Imran, and S Chiasson. What's the deal with privacy apps? A comprehensive exploration of user perception and usability. In *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia*, pages 25–36. ACM, 2015.
9. P Baker. Moral panic and alternative identity construction in Usenet. *Journal of Computer-Mediated Communication*, (1), 2001.
10. J Balicki, P Brudlo, and P Szpryngier. Crowdsourcing and volunteer computing as distributed approach for problem solving. In *Proc. of the 13th International Conference on Software Engineering, Parallel and Distributed Systems, SEPADS*, volume 14, pages 115–121, 2014.
11. Steven Bellman, Eric J Johnson, Stephen J Kobrin, and Gerald L Lohse. International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20(5):313–324, 2004.
12. C Bhagavatula, B Ur, K Iacovino, S M Kywe, L F Cranor, and M Savvides. Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. *Proc. USEC*, pages 1–2, 2015.
13. D C Brabham. Crowdsourcing as a model for problem solving: An introduction and cases. *Convergence*, 14(1):75–90, 2008.
14. D Bratvold. What is crowdsourcing?, 2017. Daily Crowdsource. https://dailycrowdsource.com/" , (Accessed 18-June-2017).
15. T D Breaux, D Smullen, and H Hibshi. Detecting repurposing and over-collection in multi-party privacy requirements specifications. In *IEEE 23rd International Requirements Engineering Conference (RE)*, pages 166–175, 2015.
16. A J Campbell. Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy. *Journal of Interactive Marketing*, 11(3):44–57, 1997.
17. P Casanovas. Open source intelligence, open social intelligence and privacy by design. In *ECSI*, pages 174–185, 2014.
18. J Cheng, C Danescu-Niculescu-Mizil, and J Leskovec. Antisocial behavior in online discussion communities. *arXiv preprint arXiv:1504.00680*, 2015.
19. T Chesney, I Coyne, B Logan, and N Madden. Griefing in virtual worlds: causes, casualties and coping strategies. *Information Systems Journal*, 19(6):525–548, 2009.
20. T C-H Cheung, H Cheung, and K-P Mark. A study of the impact of a crowd wisdom online learning community platform on student learning. In *PACIS*, page 266, 2014.

21. D Christin, A Reinhardt, S S Kanhere, and M Hollick. A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*, 84(11):1928–1946, 2011.
22. L Cilliers and S Flowerday. Information security in a public safety, participatory crowdsourcing smart city project. In *World Congress on Internet Security (WorldCIS)*, pages 36–41, 2014.
23. B Y Clark, N Zingale, and J Logan. Intelligence and Information Gathering Through Deliberative Crowdsourcing. *Journal of Public and Nonprofit Affairs*, 3(1):55–78, 2016.
24. G D Clark and J Lindqvist. Engineering gesture-based authentication systems. *IEEE Pervasive Computing*, 14(1):18–25, 2015.
25. J F De Cunha and T Galvão. State of the art and future perspectives for smart support services for public transport. In *Service Orientation in Holonic and Multi-Agent Manufacturing and Robotics*, pages 225–234. Springer, 2014.
26. C C Demchak and K D Fenstermacher. Institutionalizing behavior-based privacy. *Administration & Society*, 41(7):783–814, 2009.
27. T Dinev and P Hart. Internet privacy concerns and their antecedents-measurement validity and a regression model. *Behaviour & Information Technology*, 23(6):413–422, 2004.
28. V Dragos and K Rein. What's in a message? Exploring dimensions of trust in reported information. In *19th International Conference on Information Fusion (FUSION)*, pages 2125–2132. IEEE, 2016.
29. Elyas Esnaashari. Users' decisions about the security of mobile applications. Master's thesis, Aachen University, 2014.
30. N Fenton. Effective bayesian modelling with knowledge before data. *Retrieved April*, 29:2015, 2014.
31. R L Fogues, P K Murukannaiah, J M Such, and M P Singh. Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 24(1):5, 2017.
32. Organisation for Economic Co-operation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD, 1981.
33. A Forte, N Andalibi, and R Greenstadt. Privacy, anonymity, and perceived risk in open collaboration: A study of tor users and wikipedians. In *CSCW*, pages 1800–1811, 2017.
34. A Friedman, B P Knijnenburg, K Vanhecke, L Martens, and S Berkovsky. Privacy aspects of recommender systems. In *Recommender Systems Handbook*, pages 649–688. Springer, 2015.
35. C Fu, Z Shaobin, S Guangjun, and G Mengyuan. Crowdsourcing leakage of personally identifiable information via sina microblog. In *International Conference on Internet of Vehicles*, pages 262–271. Springer, 2014.
36. E Galinsky. The study of children in family child care and relative care–key findings and policy recommendations. *Young Children*, 50(1):58–61, 1994.
37. M Gander, C Sauerwein, and R Breu. Assessing real-time malware threats. In *Software Quality, Reliability and Security-Companion (QRS-C), 2015 IEEE International Conference on*, pages 6–13, 2015.
38. M Guzdial, B Harrison, B Li, and M Riedl. Crowdsourcing open interactive narrative. In *Foundations of Digital Games Conference June 22 - June 25, Pacific Grove, CA*, 2015.
39. C Hardaker. Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions. *Journal of Politeness Research*, 6(2):215242, 2010.
40. C Holmgård, A Liapis, J Togelius, and G N Yannakakis. Generative agents for player decision modeling in games. In *Foundations of Digital Games Conference. Ft. Lauderdale, FL*, 2014.

41. U Holtgrewe. New new technologies: the future and the present of work in information and communication technology. *New technology, work and employment*, 29(1):9–24, 2014.
42. J Howe. The rise of crowdsourcing. *Wired magazine*, 14(6):1–4, 2006.
43. D Iren and S Bilgen. Cost of quality in crowdsourcing. *Human Computation*, 1(2):283–314, 2014.
44. Q Ismail, T Ahmed, A Kapadia, and M K Reiter. Crowdsourced exploration of security configurations. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 467–476. ACM, 2015.
45. C Jensen and C Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 471–478. ACM, 2004.
46. C Jensen, C Potts, and C Jensen. Privacy practices of internet users: self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1):203–227, 2005.
47. R Kang, S Brown, L Dabbish, and S Kiesler. Privacy attitudes of mechanical turk workers and the us public. In *Symposium on Usable Privacy and Security (SOUPS)*, 2014.
48. R Kang, S Brown, and S Kiesler. Why do people seek anonymity on the internet?: informing policy and design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2657–2666. ACM, 2013.
49. G T Kishi, J G McLean, C A Pickover, and D J Winarski. Virtual avatar authentication, May 2 2017. US Patent 9,641,507.
50. A Kobsa, B P Knijnenburg, and B Livshits. Let's do it at my place instead?: attitudinal and behavioral study of privacy in client-side personalization. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 81–90. ACM, 2014.
51. S T K Lam, A Uduwage, Z Dong, S Sen, D R Musicant, L Terveen, and J Riedl. Wp: clubhouse?: an exploration of wikipedia's gender imbalance. In *Proceedings of the 7th international symposium on Wikis and open collaboration*, pages 1–10. ACM, 2011.
52. Shyong Tony K Lam, Anuradha Uduwage, Zhenhua Dong, Shilad Sen, David R Musicant, Loren Terveen, and John Riedl. Wp: clubhouse?: an exploration of wikipedia's gender imbalance. In *Proceedings of the 7th international symposium on Wikis and open collaboration*, pages 1–10. ACM, 2011.
53. J Lin, S Amini, J I Hong, N Sadeh, J Lindqvist, and J Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 501–510. ACM, 2012.
54. D Malandrino, A Petta, V Scarano, L Serra, R Spinelli, and B Krishnamurthy. 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*, pages 279–284. ACM, 2013.
55. T Minkus and N Memon. Leveraging personalization to facilitate privacy, 2014. https://ssrn.com/abstract=2448026 or http://dx.doi.org/10.2139/ssrn.2448026 Accessed 27 June 2018.
56. D Mitropoulos and D Spinellis. Securing e-voting against MITM attacks. In *13th Panhellenic Conference on Informatics. Corfu Island*, 2009.
57. D Monticolo, TK Chang, and Lahoud. An agent based approach to annotate ideas during creativity challenges in an engineering school of innovation. In *Proceedings from the First International Workshop on Educational Knowledge Management (EKM 2014),*

Linköping, November 24, number 104, pages 11–18. Linköping University Electronic Press, 2014.
58. M Netter, S Herbst, and G Pernul. Interdisciplinary impact analysis of privacy in social networks. In *Security and Privacy in Social Networks*, pages 7–26. Springer, 2013.
59. R Pandita, X Xiao, W Yang, W Enck, and T Xie. WHYPER: Towards Automating Risk Assessment of Mobile Applications. *USENIX Security*, 13(20), 2013.
60. S Patil and A Kobsa. Privacy considerations in awareness systems: designing with privacy in mind. In *Awareness Systems*, pages 187–206. Springer, 2009.
61. T Petsas, G Tsirantonakis, E Athanasopoulos, and S Ioannidis. Two-factor authentication: is the world ready?: quantifying 2FA adoption. In *Proceedings of the Eighth European Workshop on System Security*, page 4. ACM, 2015.
62. M Potthast, B Stein, and R Gerling. Automatic vandalism detection in Wikipedia. In *European Conference on Information Retrieval*, pages 663–668. Springer, 2008.
63. J Ren, Y Zhang, K Zhang, and X Shen. Exploiting mobile crowdsourcing for pervasive cloud services: challenges and solutions. *IEEE Communications Magazine*, 53(3):98–105, 2015.
64. J G P Rodrigues, A Aguiar, and J Barros. Sensemycity: Crowdsourcing an urban sensor. *arXiv preprint arXiv:1412.2070*, 2014.
65. H Rosoff, J Cui, and R S John. Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. In *SOUPS*, pages 175–186, 2014.
66. A Sárkány, Z Tősér, A L Verő, A Lőrincz, T Toyama, E N Toosi, and D Sonntag. Maintain and improve mental health by smart virtual reality serious games. In *International Symposium on Pervasive Computing Paradigms for Mental Health*, pages 220–229. Springer, 2015.
67. P Shachaf and N Hara. Beyond vandalism: Wikipedia trolls. *Journal of Information Science*, 36(3):357–370, 2010.
68. Kim Bartel Sheehan. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13(4):24–38, 1999.
69. SimilarWeb. Top websites ranking, 2018. https://www.similarweb.com/top-websites Accessed 28 June 2018.
70. D J Solove. *Understanding Privacy*. Harvard University Press, 2008.
71. R Sommerard and R Rouvoy. Towards privacy-preserving data dissemination in crowdsensing middleware platform. In *11èmes journées francophones Mobilité et Ubiquité (UbiMob'16)*, page 6, 2016.
72. J Son and J T Seo. A hybrid trust management framework for vehicular social networks. In *Computational Social Networks: 5th International Conference, CSoNet 2016, Ho Chi Minh City, Vietnam, August 2-4, 2016, Proceedings*, volume 9795, page 214. Springer, 2016.
73. R Spinelli. The value of privacy: concerns, attitudes, behaviors online, and information protection measures, 2015. http://elea.unisa.it/handle/10556/1920.
74. D M Stevenson and J Pasek. Privacy concern, trust, and desire for content personalization. In *TPRC 43: The 43rd Research Conference on Communication, Information and Internet Policy Paper*, 2015.
75. James Surowiecki. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few*. Abacus, 2005.
76. M Volkamer, K Renaud, O Kulyk, and S Emeröz. A socio-technical investigation into smartphone security. In *International Workshop on Security and Trust Management*, pages 265–273. Springer, 2015.
77. Y Wang. Privacy-enhancing technologies. In *Handbook of research on social and organizational liabilities in information security*, pages 203–227. IGI Global, 2009.

78. Y Wang, X Jia, Q Jin, and J Ma. Mobile crowdsourcing: framework, challenges, and solutions. *Concurrency and Computation: Practice and Experience*, 29(3), 2017.
79. F Wolf, R Kuber, and A J Aviv. Preliminary findings from an exploratory qualitative study of security-conscious users of mobile authentication. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*. USENIX Association, 2016.
80. D Yang, G Xue, X Fang, and J Tang. Crowdsourcing to smartphones: incentive mechanism design for mobile phone sensing. In *Proceedings of the 18th annual international conference on Mobile computing and networking*, pages 173–184. ACM, 2012.
81. K Yang, K Zhang, J Ren, and X Shen. Security and privacy in mobile crowdsourcing networks: challenges and opportunities. *IEEE Communications Magazine*, 53(8):75–81, 2015.
82. B Ye, Y Wang, and L Liu. Crowd trust: A context-aware trust model for worker selection in crowdsourcing environments. In *Web Services (ICWS), 2015 IEEE International Conference on*, pages 121–128. IEEE, 2015.
83. X Yin, W Liu, Y Wang, C Yang, and L Lu. What? How? Where? A survey of crowdsourcing. In *Frontier and Future Development of Information Technology in Medicine and Education*, pages 221–232. Springer, 2014.
84. M-C Yuen, I King, and K-S Leung. A survey of crowdsourcing systems. In *IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom)*, pages 766–773, 2011.
85. S Zogaj, U Bretschneider, and J M Leimeister. Managing crowdsourced software testing: a case study based insight on the challenges of a crowdsourcing intermediary. *Journal of Business Economics*, 84(3):375–405, 2014.
86. Y Zurynski. Writing a systematic literature review: Resources for students and trainees, 2014. Australian Paediatric Surveillance Unit. http://www.apsu.org.au (Accessed 18-June-2017).