Privacy Practices, Preferences, and Compunctions: WhatsApp Users in India

J. Dev, S. Das and L Jean Camp

Indiana University Bloomington
e-mail: jdev@iu.edu, sancdas@iu.edu, ljcamp@indiana.edu

Abstract

WhatsApp messaging platform incorporates features that pose privacy challenges, including Last Seen, Live Location, and personal profile information. The largest population of mobile messaging applications users in India use WhatsApp. Yet research on Indian perspectives towards privacy and security in social networking platforms is sparse. We queried privacy attitudes and behaviours of 213 Indian participants, using both open and closed-ended questions. The majority of participants reported that they actively use the privacy controls on multiple data types, especially in group communications. Note that, in India, groups are common not just is social settings but also in schools and workplaces. A comparison with the results of a prior study of Saudi Arabian participants shows significant overlap in access control, with more Saudis expressing concerns about being contacted by strangers. We consider our findings and propose recommendations like including more refined access control and specific culturally sensitive privacy defaults.

Keywords

WhatsApp, Social and Cultural effects, Social Media, Usable Privacy and Security, Accessibility.

1 Introduction

WhatsApp blurs the gap between social networking and traditional messaging services, allowing communication among multiple users by simplifying group communication and broadcasting messages. Consequently, it has privacy settings in place for its various features. For example, WhatsApp allows privacy control by restricting information access from 'Everyone' to 'My Contacts' for individual users. WhatsApp was designed in the US and owned by Facebook, yet India is home to the largest number of active users of WhatsApp in South-east Asia, counting over 200 million active users as of February 2017 (Singh 2017). Our goal is a culturally grounded understanding of privacy perceptions, including those of recently added features, in the under-studied population of Indian nationals. User studies have identified privacy concerns, and a similar study which focused on the Saudi users found that Saudi women had particular concerns about stranger contact (Rashidi *et al.* 2016).

WhatsApp already has controls including security notifications, end-to-end encryption and two-step authentication PIN for enhanced privacy (WhatsApp Security, 2018). Yet privacy depends on settings and user practices. (De Luca *et al.* 2016) and this

affects the user's usage decisions for a Mobile Instant Messaging (MIM) platform. Our results identify concerns, some of them more relevant to specific demographics, and we offer recommend privacy preserving practices in the platform. The goal of this paper is a more nuanced understanding of the privacy concerns for different cultural groups on a global platform. These recommendations are also immediately actionable implementations for WhatsApp designers to support the privacy requirements for diverse users.

2 Related Work

Our research was grounded in a similar study investigating the Saudi Arabian users of WhatsApp (Rashidi et al. 2016). Saudi Arabia has the highest percentage of population using WhatsApp globally, at 78% compared to India at 28% (Statistica 2018). While adoption rate is higher in Saudi Arabia, WhatsApp is the dominant messaging application in India (Singh 2017). Thus, we can provide a comparison between the nation with the highest density of adoption, and the nation with the most adopters (see in Section 4).

A core motivation of our work is that privacy studies in social networking has primarily focused on 'Western, Educated, Industrialized, Rich and Democratic'(WEIRD) societies and the social networking applications used by these populations, which is culturally distinct from Asian populations (Risk 1998). For instance, privacy risk perception of American and German participants was found to be higher than their Chinese counterparts (Risk 1998). One of the factors is the presence of stricter privacy laws (Rights 1974; Bennett et al. 2018; Cornock 2018). In general, WEIRD populations are not necessarily representative of other populations in terms of behavioural research (Henrich, Heine & Norenzayan 2010), and this has been reified in research on mobile phone sharing practices in Bangladesh (Ahmed, Haque, Chen & Dell 2017). More recent research showed that nation of origin in the Indian subcontinent is a significant factor specially for mobile privacy (Sambasivan 2018). Further, WEIRD citizens are not the largest user base of WhatsApp (Statistica 2018). Prior research has showed that privacy concerns of internet users varies across different cultural and political settings as well as between people with different levels expertise (van Schaik, Jansen, Onibokun, Camp & Kusev 2018).

An early study of social media privacy attitudes and behaviour in India used a survey of 407 participants to evaluate privacy and security attitudes (Kumaraguru & Cranor 2005). The design was grounded in similar surveys that included only American participants Indian participants were found to have higher levels of trust in information disclosure in the public and private sectors, which sharply contrasted with privacy attitude of participants in the United States. In India, posting of students' grades along with their full names on physical, publicly visible departmental noticeboards is common and even those published on websites have low security (Scientific American Blog Network, 2017). The differences between countries and the lower level of privacy concern in India were further reified by cross cultural research on privacy by Wang et al. (Wang, Norice & Cranor 2011). However, research in risk perceptions on various other social media platforms (including Friendster, MySpace, and Facebook) has reported weak correlations between user's privacy choices and their online

behaviour (Risk, 1998; Acquisti & Gross 2006). Privacy preferences, measured using a standard Likert scale, were found to be significant but to have the least impact on behaviour (Garg & Camp 2013). In contrast, King, Lampinen and Smolen report privacy attitudes to be a consequence of previous events rather than overall risk perception (King, Lampinen & Smolen 2011).

Supporting this result, Lewis, Kaufman and Christakis argue that privacy behaviours are a result of 'social influence' and 'personal incentive' (Lewis, Kaufman & Christakis 2008) such as peer attitudes and cultural biases. Patil and Kobsa have similarly argued against risk perception being a primary determinant of privacy (Patil & Kobsa 2004; Kobsa, Patil & Meyer 2012). If privacy attitudes are primarily a function of cultural attitudes, then examination of privacy in different cultures is needed to provide a more comprehensive support for different populations of customers.

Privacy concerns vary based on data type as well as data content. For example, perception and valuation of location sharing as a privacy risk vary across contexts and between individuals, and nations (Consolvo *et al.* 2005; Cvrcek, Kumpost, Matyas & Danezis 2006). Consistently studies of WEIRD populations across a range of demographics have found that data recipient and data type is a stronger factor in privacy concerns, not the generic preferences of the sender (Patil & Lai 2005; Lorenzen-Huber, Boutain, Camp, Shankar &Connelly 2011). These results motivated our inclusion of demographic and student status as questions in our study design, as described below in Section 3. WhatsApp accounts are connected to mobile numbers of individual users which itself is potentially privacy-sensitive data type, given that these numbers in India are further linked with important identifiable data including name but often extending to voter identification and financial credentials (Jain, Jain & Kumaraguru 2013).

In summary, previous research work indicates that the specific data shared by WhatsApp may have privacy concerns and further that these concerns may be different in India than in WEIRD populations. Both related work and marketplace realities argue for the importance of citizens of India as participants in research in the specific case of WhatsApp.

3 Method

Our inquiry was grounded in survey questions that have previously been asked in studies of privacy and social media extended to address the specific case of WhatsApp in India. We investigate how participants perceive and manage privacy. Our study population comprised of people who explicitly self-identify as Indian and use WhatsApp. Our core research questions are the following:

RQ1: What privacy concerns do Indians express about MIM platforms?

RQ2: How do features and demographics affect privacy preferences in MIM platforms?

RQ3: How new features impact the acceptability of MIM platforms?

RQ4: How are one-sided connections perceived by the MIM users?

The survey purposefully echoes the one used in a study of privacy concerns conducted with WhatsApp users in the Saudi Arabian population (Rashidi *et al.* 2016). The current version of WhatsApp has integrated a few of the recommendations suggested by the Saudi participants, particularly more granular access control (Rashidi et al. 2016). We evaluated whether these recommendations were applicable in the culturally different Indian population by inquiring about familiarity and use. In addition to new privacy controls, we also explored the extent to how new features, specifically Live Location, have been received and whether these have resulted in new privacy concerns.

There was a total of 83 questions, including the study information sheet, two pre-screening questions, two attention verification questions, and questions relevant to WhatsApp usage. Fifteen additional questions focus on demographics and general technology use. The demographic questions included standard questions as used in privacy for WEIRD populations: age, income, education, and employment status. The WhatsApp questions were divided into four basic mobile phone specific questions, four general questions regarding WhatsApp including news of Facebook acquiring WhatsApp, five WhatsApp usage frequency information related questions, and 26 questions about individual features. The features that we asked about were Auto-Download, Chat Backup, Read Receipts, Live Location and Status. In addition, there were 23 questions regarding user privacy concerns, privacy settings, and general WhatsApp settings questions. The remaining three questions asked about how much the participants liked or disliked certain features. The survey was distributed through snowball sampling to Indian WhatsApp users living both in India and abroad. We received a total of 454 self-reported answers from participants who use mobile messaging, of which 213 were WhatsApp users from India. Sixty-four percent were male, with more than half having at least a bachelor ‘s degree. Single people were also significantly over-represented at 76%. Participants were equally divided into students and non-students; meaning students were significantly over-represented.

4 Results and Analysis

The analysis presented in this work combines complementary qualitative results and quantitative analysis. The qualitative results allow individuals to express their concerns in their own words. The quantitative analysis enables explicit comparisons which can be used to reject specific hypotheses and compare aggregate results. As determined by previous surveys, WhatsApp is indeed widely used, with 74.65% participants reporting usage at least once a day. Unsurprisingly, the primary reason for adopting WhatsApp is because it is used by friends and family. Community perception was another reason; WhatsApp has millions of downloads with high ratings, good reviews, and a strong positive reputation. This is unsurprising, as popularity as a driving force for selecting apps has been repeatedly reported in empirical analyses of app selection (e.g., Chia, Yamamoto & Asokan 2012). Ease of

use, overall functionality, and low cost were also popular reasons for use reported by our participants.

We asked about general sensitivity of features and use of settings. In terms of *feature sensitivity*, participants described their use and expressed concern about specific features and the data shared by those features. One repeated theme was that content is being harvested from messages: 'My major concern is privacy and usage of personal chats to target advertisements to the people'. Another participant mentioned: '... things I have written (about) on WhatsApp such as clothing, shoes, travel holidays, appear next day on my Facebook ads feed'. Participants had a sense of privacy breach even though WhatsApp offers end-to-end message encryption. Feature specific usage statistics and privacy concerns are as follows.

We inquired about specific features in addition to general concern. The use of Chat *Backup*, which arguably lessons privacy, and *Blocking*, which increases it, were both reported by a super-majority of users. Arguably, the 75.12% who use *Chat Backup* feature, which indicates that they value the ability to retrieve data if lost. This echoes previous qualitative work on two-factor authentication tokens that illustrated denial of access to data is a greater concern than privacy and security (Das, Dingman & Camp 2018). *Blocking* prevents others from contacting them individually and was used 73.24% of participants. The major reasons for doing this were reported as previously disturbing inter-actions (26.83%), unfamiliarity (19.82%), an end to previous relationships (either romantic or friendship) (15.24%), and personal conflict (13.41%). Lack of reciprocity in information disclosure (refusal to show profile components like profile photo and status) was a factor for some (12.50%) of the participants. Some simply stated their refusal to contact (12.20%) specific people without additional details. Fifty-three (24.88%) participants reported that they did not block anyone.

Muting is the most widely used, with 88.73% participants reports its use in different groups. Only one participant was unaware of this feature. *Muting* is more socially complex than *Blocking*, as discussed in the analysis section.

A similar supermajority majority of participants have switched off *Auto Download* (72.77%). This could indicate concerns about privacy, intrusion upon personal space, security, cost of mobile data, or concerns about media storage. Of the participants who report that they disabled *Auto Download*, for 73.55% reported that the dominant reason was to avoid receiving media from group chats. Others were unwilling to download media from specific people or groups.

Location is consistently identified as a privacy issue across cultures. Yet 73.24% of our participants report having shared their location over WhatsApp, only 25.82% never shared their location, while nineteen people (0.94%) were unaware that the feature existed. Additionally, WhatsApp has added a new feature called *Live Location* which allows users to share their live location (precision within 100 meters) for either 15 minutes, one hour or eight hours. Nearly half (46.51%) of the participants report that they do not need to hide their *Live Location*. Most respondents report not changing any privacy settings when the *Live Location* feature was introduced (80.73%), even though it requires that the users change their phone location settings

from *Only while using the app* to *Always*. This is quite different than the location settings from the Saudi Arabian population.

As with previous work, our participants were especially concerned about their privacy in groups and suggested being able to "leave (a) group without alerting others". This is confirmed by the overwhelming number of participants who use the Mute feature (88.73%) to mute group conversations, but do not leave the group. WhatsApp creates a group notification whenever a user who leaves a group. Participants also indicated restricting Auto-download. 73.74% respondents also said that they "block (individuals) who try to contact them beyond groups, shown in Figure 2(right). Participants in the survey indicated that they want to be asked before being added to a group (72.30%) or at least otherwise asked before being added to specific groups (13.15%). This was quite similar to Saudi participants.

WhatsApp users have reported varying profile feature settings across communication recipients. Profile information includes *Profile Photo*, *About*, *Read Receipts*, *Last Seen* and *Status*. *About* is a feature that allows users to add a 140-character description of themselves. *Read Receipts* allow others who have a user's phone number to know if they have viewed their messages, in the form of checkmarks. A single check mark means that the message is sent, a double check mark means that the message is delivered, and double blue check mark on a message means that the message has been viewed by the receiver. *Status* allows users to add pictures, videos, texts about. Most of our participants report no concern about sharing information and using features for those in their contact list. A counter example was those people not willing to share *Last Seen* with anybody. We see a greater comfort of sharing details and willingness to share *Profile Photo* and *About*.

Concern about use of features was correlated. *Asking before addition* to a group is positively correlated with *blocking, disabling auto-download, muting and turning off last seen*. Thus, there is a consistency in individual privacy among users in both one-on-one and group communication. People who express the belief that some features invade their privacy choose to *hide status, profile photo, last seen* and *social relationships*. In addition, such concern is correlated with the refusal to use read receipts, as can be seen in Figure 1.

From the correlation matrix between privacy concern of users and features they use, as shown in Figure 1, we observe that people who are highly concerned about being contacted by strangers over WhatsApp are highly correlated (0.28) with people who use blocking feature and with people who are frequently contacted by strangers.

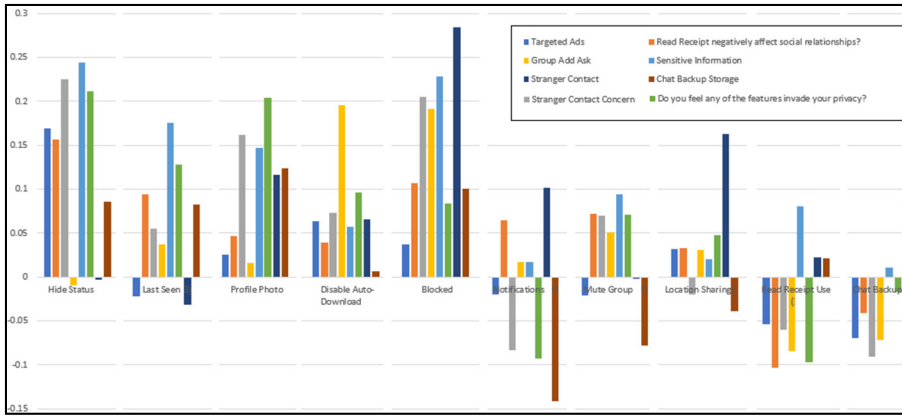

Figure 1: Privacy Concern vs Feature Correlation

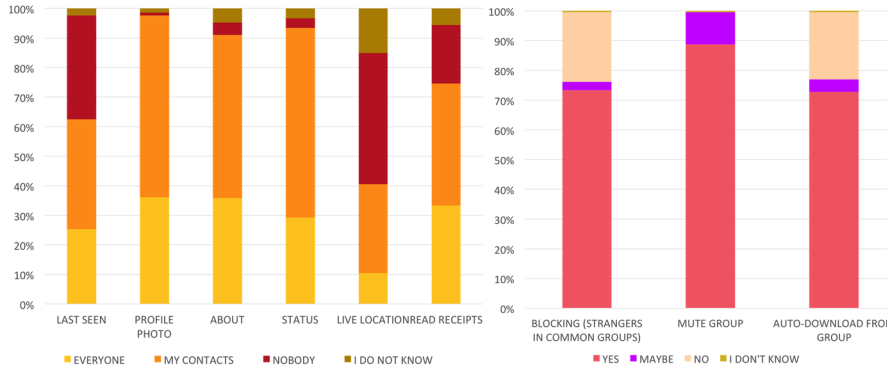

Figure 2 : Audience and Group Settings across WhatsApp (left – What are your audience settings for each of the following features; right – Do you use the Blocking/Mute/Auto-Download feature?)

5 Recommendations

Essentially our recommendations are to improve access control and to communicate risks more clearly. WhatsApp can be more privacy-preserving by allowing users to create specific trusted groups among contacts to view status and other sensitive information, while blocking it for others. In particular, groups are problematic.

Enhance Group Controls: Over 13% of participants have specific groups that they do not want to participate in. We recommend settings that allow users to be invited to a group, instead of being directly added, and giving the control to them of choosing whether to be a part of the group. Additionally, when a user is in a group with the individual who was blocked by them, the blocked can still view your messages and information, including Live Location, which requires correct implementation of exception lists. WhatsApp already incorporates exception lists to selectively choose participants who receive a user's status updates. However, it does not yet have exception lists within groups for individuals. Another feature that was specifically suggested would be the ability to leave a group without alerting others. Given proliferation of targeted and sometimes hostile political discourse on social networking platforms across the world, including WhatsApp in India, there is an argument for importance and urgency.

Bundle Settings: As observed earlier, privacy concerns about certain features are strongly linked with one another. For example, people who believe that certain features invade their privacy, hide their profile photo, status and location. Making bundles of actions to enable privacy can create a situation where WhatsApp more seamlessly address privacy concerns, particularly for users who share sensitive information. The current bundle does not seem to address expressed wishes.

Communicate privacy more clearly through reminders: Multiple participants expressed concerns about privacy preservation of the content of their messages in WhatsApp. The heuristic for the design of anonymous systems "*Say why, not how*" applies here (Norcie, Blythe, Caine & Camp 2014). End-to-end encryption in WhatsApp is a significant security benefit, but awareness among those who have adopted the technology was surprisingly low. To address the preferences of such participants, WhatsApp could provide an occasional, concise risk audit that would be technically meaningful to the user.

Integrate cultural differences and data sensitivity: The analysis of perceptions and concerns of Indians who use WhatsApp found high levels of similarities with WEIRD populations on the decision variables (trust in community, ratings, and reputation) for the selection of an application. Previous work which identified data type and data recipient as dominate factors in privacy concern in WEIRD populations (Risk 1998) were also present in these results for Indian users. However, a greater concern was reflected when users were part of a community, especially in groups, which is also reflected in the reluctance of participants to share certain data types with certain audience as shown in Figure 2 (left).

WhatsApp is used in occupational and education environments more widely in India than in the western nations. *Read receipts* carry a different connotation when there are significant power differentials between the people demanding a receipt and the person providing it. *Modifiable read receipts* were a thus, a repeated request, for plausible deniability of having read a message. Also, participants were inclined to be more socially conscious as they suggested *chat deletion without the receiver's knowledge* in groups. This message recall feature has already been implemented in updated versions of WhatsApp as of February 2018. Participants also recommended periodic deletion

of chats, which has been reflected in the fact that majority of users switched off auto-download, especially for group chats.

We acknowledge there are limitations to this study. We focused on Indian WhatsApp users. Since our primary motive was to understand the privacy concerns of active users, our participants do not include participants who do not use WhatsApp. People with greater privacy concerns might disproportionately opt out or discontinue use of WhatsApp, which was out of scope for this study. Additionally, snowball sampling was the initial method for participant recruitment, which to a certain extent, influences inter-relation between participants.

6 Conclusion

It is simple to argue that WhatsApp should not reveal too much information without proper knowledge and consent of the users; to understand the privacy preserving limit, actually doing so a major challenge. This paper is a contribution to a greater understanding of the balance between user experience and, system acceptability in support of that goal. Our study indicates when it comes to an MIM application like WhatsApp, Indians express high levels of privacy concern regarding the features they use. The results in this work are another indicator that location is privacy sensitive, and when possible, people do not want this shared to 'Everyone'.

One of the participants' expressed a clearer and evocative illustration of access control as social negotiation than any the authors can provide. This argument was for reciprocal access control, with an objection to an inability to automate their responses to others: "*I don't want a new feature in particular.... but want to improve the Last Seen feature. When you turn off the Last Seen feature, no one can see (it) and ……. but there are people who turn on their Last Seen when they like to stalk other people's Last Seen, which shouldn't happen. ……. I would like to improvise it too; once you select to hide your Last Seen, you cannot unhide your Last Seen for 15 days at least.*" It is thus apparent that Indian users would welcome feature improvements that considers cultural differences and integrates enhanced privacy settings in a platform like WhatsApp, which they widely use.

We did not include a recommendation for reflexive access control over time, because this is not a straight-forward technical implementation. As there are cultural sensitivities for currently implemented access control, reflexive access control in social networks where individuals have repeated interactions would no doubt multiply these. This is a rich domain for possible future work as we seek to understand how to empower individuals to obtain the information control they prefer on WhatsApp. Also, we observed that WhatsApp use varies differently across gender and has substantively different privacy concerns. We would like to make a quantitative elaboration on privacy attitude and demographic correlation in our future work.

7 Acknowledgement

This research was supported in part by the National Science Foundation under CNS 1565375, Cisco Research Support, and the Comcast Innovation Fund. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the the US Government, the National Science Foundation, Cisco, Comcast, nor Indiana University. We would also like to acknowledge the assistance of Joshua Streiff and Olivia Kenny who provided valuable feedback on the draft of this paper.

8 References

Acquisti, A. and Gross, R., 2006, June. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In International workshop on privacy enhancing technologies (pp. 36-58). Springer, Berlin, Heidelberg.

Ahmed, S.I., Haque, M.R., Chen, J. and Dell, N., 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. Proceedings of the ACM on Human-Computer Interaction, 1(CSCW), p.17.

Chia, P.H., Yamamoto, Y. and Asokan, N., 2012, April. Is this app safe?: a large scale study on application permissions and risk signals. In Proceedings of the 21st international conference on World Wide Web (pp. 311-320). ACM.

Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J. and Powledge, P., 2005, April. Location disclosure to social relations: why, when, & what people want to share. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 81-90). ACM.

Cornell Student Scrapes Indian Exam Results, Exposes the System's Flaws - Scientific American Blog Network, 2017, https://blogs.scientificamerican.com/guest-blog/cornell-student-scrapes-indian-exam-results-exposes-the-systems-flaws/, (Accessed on 06/14/2018).

Cvrcek, D., Kumpost, M., Matyas, V. and Danezis, G., 2006, October. A study on the value of location privacy. In Proceedings of the 5th ACM workshop on Privacy in electronic society (pp. 109-118). ACM.

Das, S., Dingman, A. and Camp, L.J., 2017, Why Johnny Doesn't Use Two Factor A Two-Phase Usability Study of the FIDO U2F Security Key. In Pre-proceedings of Financial Cryptography and Data Security 2018.

De Luca, A., Das, S., Ortlieb, M., Ion, I. and Laurie, B., 2016, June. Expert and non-expert attitudes towards (secure) instant messaging. In Symposium on Usable Privacy and Security (SOUPS).

Garg, V. and Camp, L., 2013. Ex ante vs. ex post: Economically efficient sanctioning regimes for online risks. SSRN Electronic Journal.

Henrich, J., Heine, S.J. and Norenzayan, A., 2010. Most people are not WEIRD. Nature, 466(7302), p.29.

Jain, P., Jain, P. and Kumaraguru, P., 2013, October. Call me maybe: Understanding nature and risks of sharing mobile numbers on online social networks. In Proceedings of the first ACM conference on Online social networks (pp. 101-106). ACM.

King, J., Lampinen, A. and Smolen, A., 2011, July. Privacy: Is there an app for that?. In Proceedings of the Seventh Symposium on Usable Privacy and Security (p. 12). ACM.

Kobsa, A., Patil, S. and Meyer, B., 2012. Privacy in instant messaging: An impression management model. Behaviour & Information Technology, 31(4), pp.355-370.

Kumaraguru, P. and Cranor, L.F., 2005. Privacy indexes: a survey of Westin's studies. (CMU-ISRI-5-138), Technical report, Institute for Software Research International, Carnegie Mellon University , Pittsburgh, PA

Lewis, K., Kaufman, J. and Christakis, N., 2008. The taste for privacy: An analysis of college student privacy settings in an online social network. Journal of Computer-Mediated Communication, 14(1), pp.79-100.

Lorenzen-Huber, L., Boutain, M., Camp, L.J., Shankar, K. and Connelly, K.H., 2011. Privacy, technology, and aging: a proposed framework. Ageing International, 36(2), pp.232-252.

Norcie, G., Blythe, J., Caine, K. and Camp, L.J., 2014, February. Why Johnny can't blow the whistle: identifying and reducing usability issues in anonymity systems. In Proceedings 2014 Workshop on Usable Security. https://doi. org/10.14722/usec.

Patil, S. and Kobsa, A., 2004, September. Instant messaging and privacy. In Proceedings of HCI (Vol. 4, pp. 85-88).

Patil, S. and Lai, J., 2005, April. Who gets to know what when: configuring privacy permissions in an awareness application. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 101-110). ACM.

Rashidi, Y., Vaniea, K. and Camp, L.J., 2016. Understanding Saudis' privacy concerns when using WhatsApp. In Proceedings of the Workshop on Usable Security (USEC'16).

Rights, F.E., 1974. Privacy Act of 1974, 20 U. SC § 1232g.

Risk, T.P., 1998. Cross-cultural differences in risk perception. Management Science, 44(9), p.1205.

Singh, M., 2017, 'Whatsapp hits 200 million active users in India', http://mashable.com/2017/02/24/whatsapp-india-200-million-active-users/Dka5Ao6c5sqW, (Accessed on 05/10/2018)

Statistica, 2018, 'Share of population in selected countries who are active whatsapp users as of 3rd quarter 2017', https://www.statista.com/statistics/291540/mobile-internet-user-whatsapp/, (Accessed on 05/10/2018)

Ur, B. and Wang, Y., 2013, May. A cross-cultural framework for protecting user privacy in online social media. In Proceedings of the 22nd International Conference on World Wide Web (pp. 755-762). ACM.

van Schaik, P., Jansen, J., Onibokun, J., Camp, J. and Kusev, P., 2018. Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Computers in Human Behavior, 78, pp.283-297.

Wang, Y., Norice, G. and Cranor, L.F., 2011, June. Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. In International Conference on Trust and Trustworthy Computing (pp. 146-153). Springer, Berlin, Heidelberg.

WhatsApp Security, 2018, https://www.whatsapp.com/security/. (Accessed on 04/18/2018).

Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Sanely, L., Matthews, T., Consolvo, S., and Churchill, E., 2018 August. In Symposium on Usable Privacy and Security (SOUPS).