Lessons Learnt from Comparing WhatsApp Privacy Concerns Across Saudi and Indian Populations

Jayati Dev, *Indiana University;* Pablo Moriano, *Oak Ridge National Laboratory;*
L. Jean Camp, *Indiana University*

https://www.usenix.org/conference/soups2020/presentation/dev

This paper is included in the Proceedings of the
Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

Open access to the Proceedings of the
Sixteenth Symposium on Usable Privacy
and Security is sponsored by USENIX.

Lessons Learnt from Comparing WhatsApp Privacy Concerns Across Saudi and Indian Populations

Jayati Dev
Indiana University
Bloomington, IN, USA
jdev@iu.edu

Pablo Moriano*
Oak Ridge National Laboratory
Oak Ridge, TN, USA
moriano@ornl.gov

L. Jean Camp
Indiana University
Bloomington, IN, USA
ljcamp@indiana.edu

Abstract

The purpose of this study is to understand the privacy concerns and behavior of non-WEIRD populations in online messaging platforms. Analysis of surveys ($n = 674$) of WhatsApp users in Saudi Arabia and India revealed that Saudis had significantly higher concerns about being contacted by strangers. In contrast, Indians showed significantly higher concerns with respect to social contact from professional colleagues. Demographics impinge privacy preferences in both populations, but in different ways. Results from regression analysis show that there are statistically significant differences between the privacy behaviors of Saudis and Indians. In both cases, privacy concerns were strongly correlated with their reported privacy behaviors. Despite the differences, we identified technical solutions that could address the concerns of both populations of participants. We close by discussing the applicability of our recommendations, specifically those on transparency and consent, to other applications and domains.

*Research performed while author was at Indiana University. This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

1 Introduction

WhatsApp is a multimedia messaging application with a range of capabilities beyond traditional text messaging: asynchronous chat, photo sharing, video sharing, synchronous voice and video chat, and location sharing [14]. WhatsApp supports two-person conversations, ad-hoc discussions, and larger long-lived structured groups. Due to the penetration of WhatsApp in several non-western countries and it being widely considered for peer-to-peer information sharing, there is an opportunity to study differences and similarities in privacy concerns across these nations and design corresponding privacy defaults for users. Here we focus on two populations where WhatsApp is the dominant social network platform: Saudi Arabia and India. We targeted the nation with the most intensive use of WhatsApp (Saudi Arabia) [33] and the nation where WhatsApp has its largest user base (India) [62]. In fact, WhatsApp is so widely used in Saudi Arabia and India that it is a frequent topic for national debate, having been condemned for being a tool for political propaganda [53] and for instigating mob violence with misinformation [60].

Prior research on social networking applications have found that privacy concerns vary significantly across nationalities [48, 69]. Yet much research has focused on WEIRD (Western, Educated, Industrialized, Rich and Democratic) populations [25]. While there have been independent studies on WhatsApp for Saudi Arabian users [57] and Indian users [18], there is not previous work that has directly compared the privacy choices of these two geographically and culturally distinct populations, without a comparison with western populations where privacy is more broadly studied. Having similar surveys about identical features with the same settings in two very different populations offers an opportunity for a comparison of privacy preferences and behaviors. Privacy concerns of non-WEIRD populations, including Saudis and Indians, are relatively understudied in comparison to WEIRD populations. Platform adoption is also different in non-WEIRD populations with WhatsApp more widely used in Saudi Arabia and India than in the United States or Europe. There is

a need for further studies to understand how origin reflects different priorities for managing boundaries in non-WEIRD populations. To the best of our knowledge, this is the first empirical study that compares users' concerns and attitudes on social networks between Saudis and Indians. To explore how privacy concerns influence privacy behavior, we formulated the following specific research questions:

RQ1: *To what extent are privacy concerns of Saudis different from Indians?*

We found that certain privacy concerns were similar between the participant groups, validating the work by Altman [7] who found similar privacy concerns across non-western cultures. For example, both populations were equally concerned about being added to conversation groups without consent. However, there were differences in other privacy concerns like being contacted by strangers (Saudis more concerned than Indians) and workplace acquaintances (Indians more concerned than Saudis). Even when nationality was the only measure of difference, these differences seemed to stem from cultural values often represented in previous research [51, 57].

RQ2: *To what extent does gender impinge on privacy concerns for both the populations?*

Gender has been found to be an important factor in privacy research since the 1980s [6, 59]. We consider gender separately to measure if it is an important factor in user privacy concern in our population samples as well. For women, the concern about being contacted by a stranger was found to be statistically significant greater for Saudis than for Indians. Conversely, concern towards being contacted by professional contacts for personal interactions is statistically significant greater for Indian women than for Saudi women.

RQ3: *How do privacy concerns affect privacy behavior for both of the populations?*

We analyzed the effect on privacy concern on selected behaviors for each of our participant groups. Privacy behavior was operationalized in terms of feature settings and profile information sharing boundaries which are common for most messaging platforms including WhatsApp.

We found that while privacy concerns did influence privacy behavior, they did so differently in the two groups. For instance, Saudi participants who expressed concerns over being contacted by strangers also reported using the blocking feature. Indian participants who had greater concerns about being added to a group chose to hide when they were last online and saw messages from others. Comparisons about the use of WhatsApp features and profile settings offers insight into if and how individuals are influenced by their nationality, and demographic differences. Informed by prior cross-cultural research on non-western populations, we contribute to the literature on (i) cross cultural concerns of mobile messaging applications, which are dominant in non-western populations and (ii) the differences in privacy behavior of these large populations driven by concerns. In addition to the specific cross-cultural studies, we also hope to contribute to the discussion about methods of research on privacy perceptions and behavior, e.g. [20, 55] by operationalizing behavior in terms of feature and profile settings. The comparison between the two populations using a similar experimental approach may provide general insights on privacy decision-making, which can further inform design considerations on platforms like WhatsApp.

We analyzed survey responses of 674 participants who self-identified as Saudis and Indians. While these participants might or might not be currently residing in the respective countries, they identify themselves as being Saudi or Indian citizens. We used snowball sampling; asking Saudis to share the survey with other Saudis and Indians to share the survey with other Indians. This helped ensure that we captured as many participants possible who were culturally homogeneous.

In the following section, we present an overview of other cross-population privacy studies. Section 3 details our recruitment, data compilation, and analysis procedures. Section 4 presents the results of the analyses of individual populations, and comparisons between them. We then discuss the implications of the results in Section 5, making recommendations for changes in WhatsApp and supporting these with our analysis. We conclude the paper in Section 6, illustrating avenues for future work.

2 Related Work

Prior work has long considered if privacy is a cultural phenomenon. As early as 1977, Altman recognized "privacy [as] a universal process that involves culturally unique regulatory mechanisms" [7]. Thus, there are aspects of privacy that are pervasive across cultures and those that are culturally distinct. However, due to the concentration of technology in western populations, practical reasons have made privacy studies to be largely geographically constrained.

For example, a study of 201 Facebook users in the United Kingdom found that participants' perceived risk of sharing information on Facebook was a significant predictor of privacy concerns and precautionary behaviors [68]. King, Lampinen and Smolen report privacy attitudes to be a consequence of previous events rather than overall risk perception [34]. Lewis, Kaufman and Christakis argue that privacy behaviors are a result of *'social influence'* and *'personal incentives'* [39] such as peer attitudes and nationality biases. This allows an opportunity to study population intrinsic privacy concerns as a predictor of privacy behavior. In privacy research, however, WEIRD populations are not necessarily representative of other populations [25]. It is reasonable to evaluate if privacy research on WEIRD populations predicts findings from South-East Asian and Middle-Eastern populations given that studies of offline risks have consistently found strong evidence that the tolerance for risk [29] and the cultural framing

of risk [9] vary significantly across nations.

2.1 Cross-Cultural Studies in Privacy

The privacy community has been increasingly interested in privacy concerns and attitudes across cultures, often comparing non-western populations against western populations like [44], [69], and [32]). Cvrcek et al.'s study of privacy valuation across Europe found significant differences between Greek, Belgian, Czech, German, and Slovak populations in terms of location privacy indicating the importance of studying culturally varied populations [17]. Further afield, privacy risk perception of German participants were found to be higher than American participants, and both were higher than their Chinese counterparts [29]. A study of 92 participants in three countries found that generally American respondents were the most privacy concerned, followed by the Chinese while Indians showed the least concern [69]. The difference in the WEIRD populations were partly credited to the presence of data protection laws, but nationality also played a role [11, 16, 47]. These smaller studies were also followed by larger studies on privacy concerns of Internet users across different cultural and political settings like [10] and [40] as well as development of universal privacy frameworks [67].

Prior work has also attempted to study individual populations in-depth in Japan [3], Saudi Arabia [1, 73], Bangladesh [4] and India [19]. If privacy attitudes are primarily a function of national attitudes, then examination of privacy in different populations is needed to provide the support for different populations. A core motivation of our work has been to contribute to this rising body of work by not only confirming that there are differences, but also confirming that there are similarities—both of which can be useful in making actionable privacy controls.

2.2 Privacy and Gender

The way different cultures treat men and women also has been found to have an effect on their privacy perceptions [7]. Historically, gender has been considered as "a key social variable in the availability of certain forms of individual and group privacy" [6]. While both men and women are equally subject to invasions of privacy, how these invasions have an effect upon them can vary. Complex gender norms can spill over to cyberspace from the physical world that have a greater impact on women than men (e.g., stalking [38, 57] and family expectations [4]). Female internet users were also "disproportionately [more] prone" to online harm since they formed the greater population of online consumers [8].

Accordingly, there have been a rising number of studies on understanding how gender impinges privacy concerns. A study on American teens found that privacy concerns about receiving unknown emails were higher for female high schoolers [72]. Similarly, greater privacy concerns in women caused them to have enhanced "privacy protection behavior" on Facebook [28]. Few studies have also been focusing on the impact of gender in non-western populations in South-east Asia [59]. An important aspect of privacy is its formulation as a form of 'modesty', where in some cultures, privacy is a way to protect what the society might objectively consider as immoral [70]. Since women tended to have greater privacy concerns and enforced privacy preserving behavior, gender was also a significant consideration in our study on Saudi and Indian populations where culture has a more patriarchal grounding [5, 54].

2.3 Privacy Behavior Against Concerns

Our third research question has been grounded in previous work on privacy behavior resulting from privacy concerns. 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 behavior [2]. Most of the users were unable to or uninterested in addressing privacy settings to control information sharing. The source of this 'privacy paradox' was investigated in a study of 232 Facebook users, where the perceived risk of sharing information was found to be the most important determinant of privacy behaviors. Privacy preferences, measured using a standard Likert scale, were found to be significant but to have the least impact on behavior [22]. These findings were also supported across cultures (e.g. China) [52].

Patil and Kobsa have similarly argued that people are more privacy concerned about specific factors like accessibility of information to strangers, content of the messages in communication, and reliability of the service [50]. Following their example, we have also considered information sensitivity and stranger contact concern as factors influencing privacy behavior. In cases where privacy protecting behaviors are present, they suggest that this is a result of *'impression management'*, specifically in messaging apps [36] at workplaces. Privacy concerns were found to vary based on data type as well as data content. For example, perceptions and valuation of location sharing as a privacy risk vary across contexts and between individuals, and nations [15]. Hence, we also consider if users were concerned with being contacted by colleagues over mobile messaging applications outside of workplace and if it changed how they managed information over messaging platforms (like restricting media download).

2.4 Mobile Messaging Platforms

In this section we discuss WhatsApp as an example of a mobile messaging platfrom. In most studies, e.g. [69], Facebook has largely been the dominant platform studied in cross-cultural privacy research. While Facebook does have a fairly large user base across countries, it is often not the dominant platform used by the majority of the population. With the rise of smartphones, mobile phone based messaging applications like WhatsApp have been increasingly adopted in non-WEIRD populations instead of Facebook [62]. One of

the countries in our study, Saudi Arabia, has the highest WhatsApp market penetration, with 78% of the population using WhatsApp [63]. WhatsApp is also treated as a credible source of information for law enforcement [42]. It is integrated into daily life, in educational institutions, political groups [12] and places of employment, making information dissemination over WhatsApp an important domain to study [13, 58]. Similarly, in India, reacting to the brutality of the photos distributed over WhatsApp, five people were incorrectly identified as kidnappers and killed by the residents of isolated towns [24]. In response, WhatsApp has implemented tagging to indicate that the message was forwarded and limited the ability to forward a specific message to five people to prevent mass forwarding [46]. Though the latter event happened after the breadth of our study, it highlights how WhatsApp is an important focal point in behavior over social media, especially for these understudied populations.

Despite the ubiquity of WhatsApp in daily life in many non-WEIRD countries, it is only recently being considered in social networking research [49]. For example, the ever popular Vinco's *Annual World Map of Social Networks* does not even consider WhatsApp as a social network, but rather as a messaging platform.[1] Given the range of services and group management functionalities of WhatsApp, privacy evaluations of social use are worthwhile. While it is true that it might not forever be the dominant messaging application in non-WEIRD countries like Saudi Arabia and India, research on privacy concerns of these populations may be applicable to competing or future platforms as well.

3 Methods

For this study, we used data collected through a survey instrument targeted at WhatsApp users, above the age of 18, who identified themselves as either Saudis or Indians based on nationality. The instrument was initially developed as a bilingual self-reported survey for Saudis in Arabic and English. We adopted the English version for the Indian population and added questions on Location and use of Live Status, but did not translate the survey into any of the major languages or dialects in India due to the fact that there are too many languages that could effect interpretation of the translated text. English is used for all official government communications in India according to the Official Languages Act of 1963 [65] which makes it convenient for population sampling. While the survey contains both quantitative and qualitative responses, we focus here on the quantitative results in order to gain empirically grounded insights of privacy concerns.

3.1 Population Sampling

WhatsApp is the most widely used instant messaging platform in both Saudi Arabia and India [33, 62]. This allowed us an opportunity for convenience sampling, given researchers from the aforementioned countries. The survey was done in two phases, the first targeted at Saudi users in 2015 and the second targeted at Indian users in 2017. The study was approved by the University's Institutional Review Board (IRB) for both surveys. We conducted snowball sampling to recruit respondents who were culturally homogeneous. It also would have been difficult and possibly infeasible to reach Saudi women with a survey distributed in the United States. We designed the second study (with Indian users) to enable comparison with the first. Given we were excluding Saudis/Indians living outside their country for years (because privacy perceptions can change depending on the country of residence) we retained the snowball sampling method for both similarity and recruitment. Since the data were collected in two phases over a gap of two years, we removed additional features available on WhatsApp to make the variables in the Saudi and Indian groups consistent, as detailed in Section 3.4. The initial survey instrument sampled 820 WhatsApp users; 452 from Saudi Arabia, 146 from non-Saudi Arabs, and 222 from India. The 146 non-Saudi Arabs were excluded from analysis, making the total number of participants 674. This was because non-Saudi Arabs can have membership from 21 Arab countries of Algeria, Bahrain, Comoros, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Qatar, Saudi Arabia, Somalia, Sudan, Syria, Tunisia, United Arab Emirates, and Yemen in addition to the Palestinian Territories. This would increase the variability since we did not have enough number of users from each of these countries. This gave us two datasets of 452 (Saudi) and 222 (Indian) users respectively.

3.2 Sample Size and Variables

Both Saudi and Indian population datasets were then combined for all 674 valid responses from users who identified themselves as Saudi or Indian nationals respectively. We had 452 Saudi participants (we needed 385 participants for a 95% confidence level and 5% margin of error) and 222 Indian participants (we needed 271 participants for a 95% confidence level and 5% margin of error). Table 1 shows the demographic distribution of both populations across gender, age and educational qualification.

Since our dataset was obtained from a prior survey of Saudi respondents that contained only binary gender, we had to remove non-binary or undeclared responses from seven users in the survey to maintain consistency. Gender categories have been a long standing debate [64] and a follow-up study that accounts specifically for privacy concern variations based on gender would be invaluable. We assigned a variable to every question in our complete dataset, resulting in 19 variables, across four categories: privacy concerns, general usage, demographics, and feature and profile information settings. The number of independent variables in the survey was 12 (Table 2 contains 11 and nationality) for consistency across variables

[1] https://vincos.it/world-map-of-social-networks/

that can be compared for analysis. Questions that were present in one dataset but absent in the other were removed. We also removed responses which had missing values for any of the questions that remained in our dataset.

Demographic Details		Saudis	Indians
Gender	Male	159	140
	Female	293	75
Age (years)	18-24	99	80
	25-30	225	123
	31-40	103	17
	41-50	21	2
	over 50	4	0
Education	High School or Less	30	4
	Some College	38	2
	Bachelors	58	90
	Masters or Professional	18	114
	Doctoral	2	9
		452	222

Table 1: Demographic distribution of the populations broken down into two samples.

Recall the three research questions were about the differences and similarities of privacy concerns (***RQ1***), how demographics impinge these concerns (***RQ2***), and how these concerns affect privacy behavior (***RQ3***). The survey had five questions for each population into the 'Privacy Concerns' category. In order to answer if these concerns were similar or different based on demographics (***RQ2***), we included demographic queries: age, gender, and education. Gender has been found to be a significant factor in use of security technology, and has a significant impact on privacy behavior [21]. Expertise has been found to be a major determinant of security behaviors [20, 56]. Expertise also clearly impinges risk awareness. The differences, or lack thereof, in privacy and security papers sometimes is embedded in expertise, such as works where student samples have predominantly male technology experts and predominantly female non-experts. However, here gender is the only explicit variable, based in no small part on the differences in findings in the comparative works discussed in Section 2. In addition a study of privacy concerns on Facebook that addressed use and risk perceptions found gender to be a significant variable in WEIRD population samples [21].

In order to measure if privacy behavior changed according to privacy concerns for each population (***RQ3***), privacy behavior of participants was operationalized as use of features on WhatsApp. This includes blocking others from accessing personal devices, and limiting the transmitting of profile information. Table 3 lists the dependent variables in our study. We have four dependent variables as 'Feature Settings'. These features include *Blocking*, *Auto Download*, *Location*, and *Notification*. The responses to feature usage questions are binary. Three additional variables for profile settings, *Profile Photo*, *Last Seen*, and *Status* were also included because they signified access control to an individual's profile at three levels - Nobody, My Contacts, and Everyone. These seven variables served as dependent variables in our study. Similarly, Table 2 lists the independent variable categories, 'Privacy Concerns', 'Usage', and 'Demographics' further described below.

1. Privacy Concern Variables: Users were queried about their privacy concerns while using WhatsApp. The survey did not contain generic questions on privacy, but specific questions in the context of WhatsApp. This, however, does not limit the questions to the existence of WhatsApp. The variables under 'Privacy Concerns' like *Sensitive Data*, *Professional Contact*, *Targeted Ads*, *Group Add Ask*, and *Stranger Contact Concern* can be applied across all mobile messaging platforms with similar functionality which ensures that questions on privacy concerns remain relevant beyond the scope of our study.

2. Usage Variables: These variables measure the usage habits of users on WhatsApp. This includes information on the operating system (*Platform*), frequency of usage (*Frequency*) and length of usage (*Length*).

3. Demographic Variables: The demographic variables we considered were *Age*, *Gender*, and level of education (*Education*).

Apart from these, we had a separate variable for nationality that distinguished between Indian and Saudi users. The list of independent and dependent variables and their relationship with the research questions we investigated in this paper are in Table 8 (Appendix).

3.3 Analysis

For our first research question (***RQ1***) we compared privacy concerns between Saudis and Indians using the Mann–Whitney–Wilcoxon (MWW) test. In doing so, we compared the responses to their privacy-related concern questions ('Privacy Concern' variables). All of the five variables were measured on a three-point Likert scale for the Saudi population. The MWW test is a non-parametric test of the null hypothesis that it is equally likely that a randomly selected value from one sample will be less than or greater than a randomly selected value from a second sample [43]. This makes it suitable for dealing for the Likert-scale data used for quantifying privacy concerns in the two samples [71].

We also use the MWW test to answer our second research question (***RQ2***) pertaining to gender differences in privacy concerns. We maintain the separation between the populations, with gender as the additional control variable.

For our third research question (***RQ3***), where we measure the concern factors that influence privacy behavior, we per-

Q. No.	Description	Type
	Privacy Concerns	
1	*Sensitive Data:* I frequently use WhatsApp to send/share private or sensitive chats/media.	Likert
2	*Professional Contact:* Do you use WhatsApp to communicate formally or informally with your professional contacts, like your boss or coworkers?	Likert
3	*Targeted Ads:* Are you concerned that since Facebook bought WhatsApp, targeted ads might start appearing in WhatsApp?	Likert
4	*Group Add Ask:* When adding me to a group chat, I would like the app to (ask/ not ask) me before adding.	Likert
5	*Stranger Contact Concern:* Are you concerned that anyone who has your phone number is able to contact you and see the activity shared publicly using WhatsApp?	Likert
	Usage	
6	*Platform:* Which operating system do you currently use for your primary smartphone?	Categorical
7	*Frequency:* On average, how often do you use WhatsApp?	Categorical
8	*Length:* How long have you been using WhatsApp?	Categorical
	Demographics	
9	Age	Categorical
10	Gender	Boolean
11	Education	Categorical

Table 2: Privacy concerns, usage and demographic factors which are independent variables for both population samples.

formed an exploratory factor analysis (EFA) along with logistic and and ordered logistic regression. EFA was used to find influential underlying factors from a set of observed independent variables. We used the Privacy Concerns, Usage, and Demographics variables to form a new set of variables that would be independent of each other. EFA extracts the maximum variance from all the variables and groups them under a common score. A latent factor representation of the independent variables allows us to deal with multicollinearity. When the degree of collinearity is high between independent variables, it becomes difficult to estimate the relationship between each independent variable and the dependent variable, as well as, the overall precision of the estimated coefficients.

EFA helps in finding the relationship between independent variables in terms of a smaller set of factors. We tested the adequacy of conducting EFA for both samples using the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy [26] and the Bartlett's test of Sphericity [66]. The KMO measure is a statistic that indicates the proportion of variance in the dependent variables that might be caused by underlying factors. The Bartlett's test of Sphericity measures the hypothesis that the correlation matrix is an identity matrix, which would indicate that the independent variables are unrelated and therefore unsuitable for EFA. We used orthogonal rotation with the varimax method to force the latent factors to remain uncorrelated. We considered an item to be loaded on a factor if its loading exceeded 0.3 and repeated it for each sample. Finally, we used logistic and ordered logistic regression to analyze the influence of the independent variables in the privacy attitudes of both samples. This results inform the discussion about how nationality-based mental models have an impact of the privacy preferences (measured through feature and profile setting choices) of users. We used the *psych* package in R to run the EFA and regression analyses.

3.4 Considerations and Limitations

In the two years between the studies there were no significant user interface changes; however, WhatsApp did add new features. These features were *Live Location* (real-time location sharing), document sharing, making phone calls, and end-to-end encryption for text messages. We have tried to account for the changes in features by measuring respondents' settings on these features independently. We acknowledge that there is a possibility of a shift in general privacy attitudes over two years of the survey. We also noted that there were no changes in WhatsApp during this time period that addresses our recommendations and yet hope that these may be adopted. WhatsApp had a $1 yearly subscription fee beginning in 2013. This was eliminated in 2016 [61] which might have an effect on its adoption in both countries.

This study is focused on participants with different origins, but not necessarily culture. The distinction between culture and origin is profoundly important, nuanced, subject to a vast literature [27]. This discussion is beyond the scope of this work but could be the subject of further research.

Due to the use of snowball sampling, our sample is not statistically representative of the populations. However, it does provide valuable insight into the privacy concerns of respondents. Snowball sampling was responsible for the demographic skew even as it helped reach our participants. De-

mographics is one of the many factors that affect findings like workplace contact concerns. It is reasonable to assert that a representative sample would include the issues we address (like the prevalent use of WhatsApp in workplaces) and our results would still hold. Nevertheless, a more representative sample that accounts for nuanced cultural differences within countries would be beneficial for further research and would likely expand the recommendations.

4 Findings

Following the quantitative analysis above, we categorized our findings in three sections. First, we report privacy concerns based on nationality. Next, we report privacy concerns based on gender. Finally, we present how privacy behavior of users was dependent on privacy concerns.

4.1 Privacy Concerns Based on Nationality

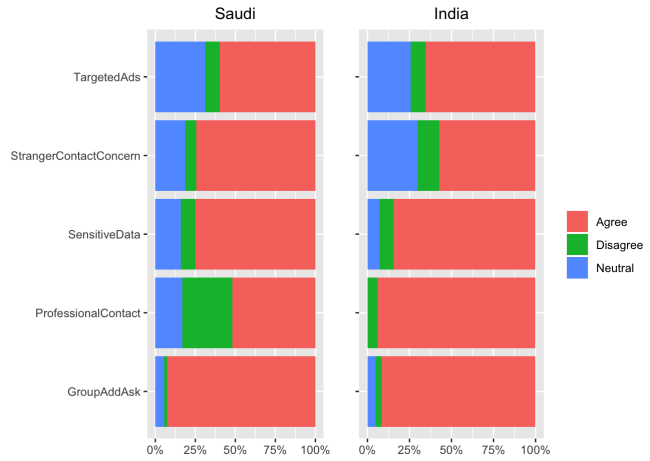
Overall, we noticed that while Saudi and Indian participants have different privacy concerns towards WhatsApp, there are concerns that are also similar for both population samples. Figure 1 shows the differences regarding the privacy concerns between Saudis and Indians. Specifically, we found that the higher concerns towards being contacted by strangers is statistically significant for Saudis than for Indians ($W = 37,254, p < .001$). On the other hand, we found that Indians tend to be more privacy concerned than Saudis regarding being contacted by professional contacts. Indian respondents also seemed to have greater privacy concerns about being subjected to targeted advertisements over WhatsApp. Concerns towards being contacted by a professional contact ($W = 66,299, p < .001$) and targeted advertisements ($W = 56,408, p < .001$) that uses data from their conversations are significantly greater for Indians than for Saudis respectively.

However, we did not find significant differences between concerns about *Sensitive Data* and *Group Add Ask*. Their concerns over sharing sensitive information and preferences for being asked before someone adds them to a group were similar. Respondents from both samples shared data which they believed was sensitive, and expressed displeasure at being added to WhatsApp groups without consent.

4.2 Privacy Concerns Based on Gender

Figure 2 compares the privacy concerns between Saudis and Indians by gender. We tested the same five categories pertaining to privacy concerns (*Targeted Ads*, *Stranger Contact Concern*, *Sensitive Data*, *Professional Contact*, and *Group Add Ask*) as seen in Table 2, splitting the two samples by gender and using the MWW test. We found that privacy concerns between genders within the same sample (for both Saudis and Indians) are not statistically significant. In other words,

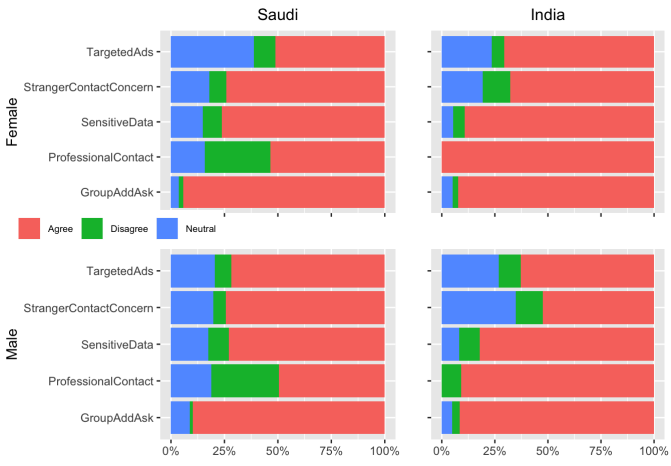
Figure 1: Privacy concerns of respondents by nationality.



within the same sample, both men and women expressed the same level of privacy concerns.

However, when we compared the two samples by gender individually, the concerns were different. For females, we found that the concern towards being contacted by a stranger is statistically significant greater for Saudis than for Indians ($W = 11,648, p = .015$). Similarly, we found that the concern towards being contacted for professional contact is statistically significant greater for Indians females than for Saudis females ($W = 6,569, p < .001$). We also compare

Figure 2: Privacy concerns of Saudi and Indian respondents by gender.



the privacy concerns between samples for males. We found that the concern towards being contacted by a stranger is statistically significant greater for Saudi males than for Indian males ($W = 12,222, p < .001$). Conversely, we found that the concern towards being contacted for professional contact is statistically significant greater for Indians than for Saudis ($W = 8,545, p < .001$). Overall, results across gen-

Q. No.	Description	Type
	Feature Settings	
1	*Blocking:* Did you use the Blocked feature in WhatsApp to block any person from contacting with you?	Boolean
2	*Auto Download:* Did you disable the auto-download feature on WhatsApp?	Boolean
3	*Location:* Have you previously shared your location using WhatsApp?	Boolean
4	*Notification:* Have you enabled WhatsApp to send you notifications when there is a new message?	Boolean
	Profile Information	
6	*Profile Photo:* What is your setting? (Everyone, My Contacts, Nobody)	Categorical
7	*Last Seen:* What is your setting? (Everyone, My Contacts, Nobody)	Categorical
8	*Status:* What is your setting? (Everyone, My Contacts, Nobody)	Categorical

Table 3: Feature settings and profile information which are dependent variables for both population samples.

ders between different samples are consistent for females and males. Thus, the privacy concerns reflected by overall participants were also reflected by gender with no gender differences within each sample.

We did not find significant differences between *Sensitive Data* and *Group Add Ask* privacy concerns when comparing genders between the two samples.

4.3 Comparing Privacy Behavior Based on Privacy Concerns

Following comparison between Saudi and Indian users of WhatsApp against their privacy concerns, we tested to see if privacy behavior in each sample differed based on privacy concerns. Privacy behavior was measured in terms of user behavior in using WhatsApp features like *Blocking* (restricting access to self), *Auto-Download* (allowing automatic download of media files), *Location* (sharing static map coordinates), and *Notification* (enabling notifications on device from WhatsApp when user receives a message). We used three additional features pertaining to user profile information - *Profile Photo*, *Last Seen* (when the user had last checked their WhatsApp messages) and *Status* (static description of users about themselves). These had three levels of access control - Everyone, Contacts only, and Nobody. We removed *Live Location* (ability to share location continuously instead of static coordinates), *Read Receipts* (blue ticks showing when messages have been delivered and seen), and *Live Status* (instant story posts visible for 24 hours) which were not present across both surveys.

4.3.1 Exploratory Factor Analysis (EFA)

Saudi Users: For Saudis, the variable to subject ratio was 1:41.1 (452/11 = 41.1). This shows that the number of participants per question was adequate to obtain quality in the factor solution [35]. The Kaiser-Meyer-Olkin (KMO) test statistic for sampling adequacy was 0.50 which makes this dataset acceptable for EFA. In addition, the Bartlett's Test of Sphericity [66] revealed that the correlation matrix came from independent samples ($\chi^2 = 177.1$, $df = 55$, $p < .05$), and further indicated that the factor analysis was justified by the properties of the correlation matrix. Therefore, EFA is considered as an appropriate technique for further analysis of this sample.

	Age & Education	Usage Platform	Group Permission	Gender	Information Sensitivity	Targeted Ads
Age	0.962					
Education	0.490					
Platform		0.992				
Group Add Ask			0.671			
Gender				0.565		
Sensitive Data					0.418	
Frequency					0.316	
Targeted Ads						0.461
Stranger Contact						
Concern						
Length						
Professional Contacts						
Eigenvalues	1.465	1.284	1.213	1.101	1.03	1.011
% of Total Variance	10.7	9.1	4.8	3.9	3.7	2.6

Table 4: Rotated varimax factors from the factor analysis of privacy concerns of Saudi participants.

We identified and extracted factors based on the Kaiser's criterion for eigenvalues, i.e., we choose all factors with an eigenvalue greater than 1 as a measure of reliability [31]. Figure 3 shows the scree plot of successive eigenvalues. Specifically, it shows that after the sixth the total variance accounts for smaller amounts. The rotated factor loadings along with the eigenvalues are illustrated in Table 4.

The six selected factors predicted 34.8% of the variance, including: variables that are related to demographics (i.e., *Age and Education*), operating system type (i.e., *Usage Platform*), privacy issues for being added to a group chat (i.e., *Group Permission*), *Gender*, privacy issues to send private data and frequency (i.e., *Information Sensitivity*), and being targeted by advertisements (i.e., *Targeted Ads*). Each of these components accounted for 10.7%, 9.1%, 4.8%, 3.9%, 3.7% and 2.6% of variance respectively.

Indian Users: For Indians, the variable to subject ratio was 1:20.1 (221/11 = 20.1). Similar to Saudi respondents, the number of participants per question was adequate to obtain quality

Figure 3: Scree plot showing eigenvalues for EFA among Saudi users. There are six values that are greater than 1.

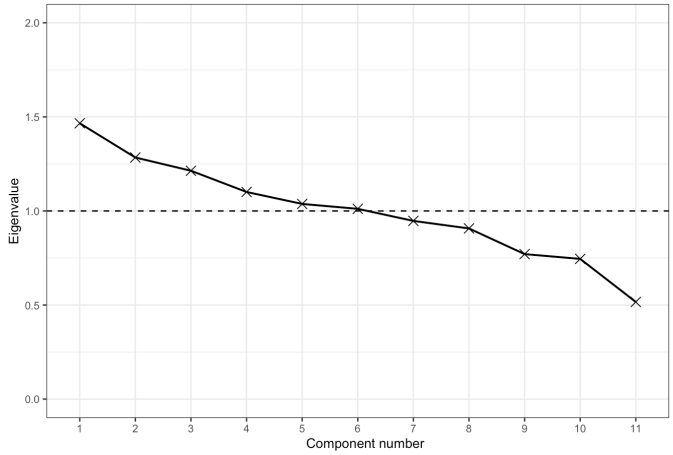
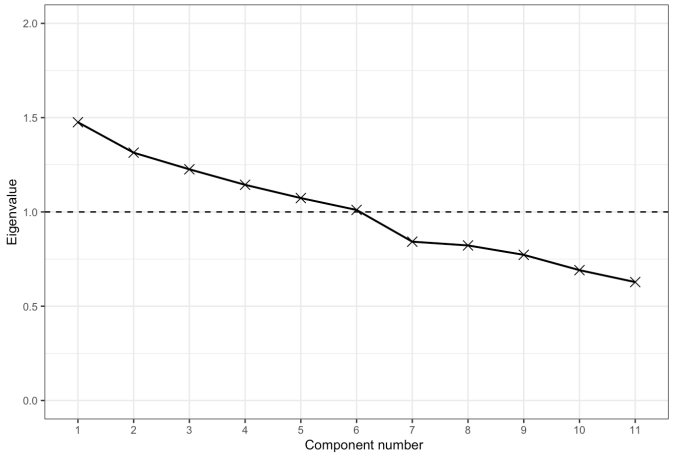


Figure 4: Scree plot showing eigenvalues for EFA among Indian users. There are six values that are greater than 1.



in the factor solution [35]. The KMO test statistic was 0.50 which makes this dataset acceptable for EFA. The Bartlett's Test of Sphericity revealed that the correlation matrix came from independent samples ($\chi^2 = 70.5$, $df = 55$, $p < .05$), and further indicated that the factor analysis was justified by the properties of the correlation matrix. Therefore, EFA is considered as an appropriate technique for further analysis of this sample as well.

We retained only the factors which had eigenvalues greater than 1 in accordance with Kaiser's criterion like we did for the Saudi samples [31]. As can be seen Figure 4 shows the scree plot of successive eigenvalues, of which we selected six factors. The rotated factor loadings are illustrated in Table 5.

The six selected factors predicted 34% of the variance, including: variables that are related to privacy regarding *Sensitive Data*, type of operating system (i.e., *Usage Platform*), frequency of using WhatsApp (i.e., *Usage Frequency*), privacy issues for being added to a group chat and education (i.e., *Education and Group Permission*), privacy issues related to being targeted by advertisements and age (i.e., *Age and Targeted Ads*), and privacy issues regarding being contacted by professional contacts (i.e., *Professional Contact*). Each of these components accounted for 9.1%, 5.8%, 5.2%, 4.7%, 4.7% and 4.5% of variance, respectively.

	Sensitive Data	Usage Platform	Usage Frequency	Education & Group Permission	Age & Targeted Ads	Professional Contacts
Professional Contact						0.676
Targeted Ads					0.609	
Age					0.340	
Group Add Ask				0.504		
Education				0.353		
Frequency			0.587			
Platform		0.741				
Sensitive Data	0.981					
Stranger Contact						
Concern						
Length						
Gender						
Eigenvalues	1.475	1.314	1.073	1.010	1.143	1.225
% of Total Variance	9.1	5.8	5.2	4.7	4.7	4.5

Table 5: Rotated varimax factors from the factor analysis of privacy concerns of Indian participants.

After EFA for each sample, we tested the six factors obtained in each case against privacy behavior of respondents.

4.3.2 Findings from Regression Analysis

We used factor scores (i.e., each example weight into its factor loading) from the EFA as the predictors of privacy attitudes using multiple logistic regression (for *Blocking*, *Auto Download*, *Location*, and *Notification*) and multiple ordinal logistic regression (for *Profile Photo*, *Last Seen*, and *Status*) based on the type of dependent variable. In doing so, each example contribution to the factor score depends on how strongly it relates with the factor. The reported regression coefficients are based on the logarithm of the odds. Odds are the probability of an event occurring divided by the probability of the event not occurring. In our results, that means that for every one unit of gain in the independent variable, the logarithm of odds of the dependent variable increases by the correspondent coefficient. For details about the interpretation of the regression coefficients, we suggest the reader the work in [23].

Saudi Users: Table 6 shows the coefficients of the regression model for Saudi respondents with statistically significant p-values. As seen in the table, most factors only effect one of the feature settings. Given that the level of significance is (*) for $p < .05$, (**) for $p < .01$, and (***) for $p < .001$, we observe the following.

Gender is statistically significant and contributes (0.498) to the overall inclination to use the *Blocking* feature. Thus, female Saudi users were more likely to use this feature to block access to them on WhatsApp if it was from a person they did not know.
When respondents were more likely to be asked before being

added to a group, the likeliness that they would not download content from another user was higher, indicated by a high coefficient in case of *Auto Download* (0.416) (note that the question for *Auto Download* is framed in terms of disabling the feature).
Age and Education (-0.2789) as well as privacy concerns about receiving targeted advertisements (-0.3067) were linked to user choice of turning notifications on or off. Older and more educated users were more likely to turn off notifications. Similarly, users with higher concerns about targeted advertisements turned their notifications off. This indicates that users who had more experience and knowledge of WhatsApp, coupled with an aversion to targeted advertisements were more likely to avoid notifications.
Privacy concerns did not significantly affect *Location* settings and profile settings like *Profile Photo*, *Last Seen*, and *Status* for Saudi users.
Usage variables like type of operating system (*Usage Platform*) did not effect privacy behavior. Similarly, willingness to share sensitive data frequently (*Information Sensitivity*) did not effect privacy behavior.

Indian Users: Table 7 shows the coefficients of regression analysis for Indian respondents. We found that privacy concerns did effect privacy behavior in case of Indian users as well, but their privacy behavior was very different from Saudis.
Privacy concerns or demographics did not effect feature settings like *Blocking* (which was effected by gender in case of Saudis) and *Location* sharing. However, unlike Saudi users, privacy concerns did effect how Indian users changed their profile settings like *Profile Photo* and *Last Seen*. *Last Seen* had a high value of regression coefficient (0.32010) and was more likely to be hidden by more educated users who were concerned about being added to a group with consent (*Education and Group Permission*). A possibility is that they chose to hide when they were last online when more people had access to them.
Privacy concerns about being contacted by colleagues from a workplace (*Professional Contact*) had a higher coefficient for *Auto Download* (0.35605) and Notification (0.420984) settings.
Similar to Saudi users, concerns about sensitive data did not play a role in effecting privacy behavior. More broadly, education and group permissions were two overlapping factors that effected privacy behavior in both samples. While gender and targeted advertisements played a more important role for Saudi users, privacy behavior of Indian users depended on professional contacts. Profile settings were effected by privacy concerns more for Indian users than Saudi users.

5 Discussion and Implications

Our findings reify and add to previous results on the relationship between culture and privacy. The major goal of this study was to highlight both similarities and differences between two culturally distinct non-WEIRD populations. Our findings expand existing literature on cross-cultural privacy in the SOUPS community. We discuss practical recommendations for more inclusive privacy design choices for non-WEIRD countries; for example, stranger contact concerns and work-personal boundaries.

We found that **participants within each individual sample had similar privacy concerns**. Neither gender nor origin alone were significant determinants; however, **gender effected privacy controls among Saudi users**. Not only did female users had greater privacy concerns about being contacted by strangers over their Indian counterparts, but also this concern effected the use of the blocking feature (to prevent strangers from contacting them).

We have also shown that privacy concerns were dependent on origin, but there were aspects common across the non-WEIRD samples in the study. **Both participant groups shared sensitive content over WhatsApp. Furthermore, this sharing was not found to have an effect on their privacy behavior**. Both groups also had similar group privacy concerns and disliked being added to a group without their consent. However, this was expressed in different ways in different samples. While Saudis restricted **content** from auto-downloading, Indians restricted **visibility access** (being seen by other people that they were online) by hiding their *Last Seen*.

In terms of privacy behavior, neither Saudi nor Indian users changed settings based on the sensitivity of information **content**, but rather information **recipient**. This was particularly true for restricting stranger contact (among Saudis) and preventing use of WhatsApp for professional contacts (among Indians).

Based on our findings, we make the following design recommendations to the already significant security and privacy features of WhatsApp (and future social messaging platforms). While these are specific to WhatsApp, the feature settings offered by WhatsApp and the privacy concern variables that have been operationalized in our study (*Targeted Ads*, *Stranger Contact Concern*, *Sensitive Data*, *Professional Contact*, and *Group Add Ask*) can be observed in other mobile messaging applications like Signal as well.

5.1 Offer an Option for Permissions-Based Contact

Being contacted by strangers was disliked by Saudi female respondents. While we do not suggest a gender-based control, adhering to stronger privacy concerns might improve the privacy of the overall platform. One of the peculiarities of WhatsApp is that contact information of users is easily accessible if they are in a common group, even after blocking particular users. A problem that might happen in large groups in that strangers can contact users over other communication

Factors	Blocking	Auto Download	Location	Notification	Profile Photo	Last Seen	Status
Intercept	1.208***	0.427***	0.722***	1.291***			
Age and Education	-0.024	0.088	-0.157	-0.279*	0.013	-0.021	-0.058
Usage Platform	-0.139	0.117	0.117	-0.217	-0.027	0.002	-0.068
Group Permission	0.173	0.416***	0.034	-0.241	-0.109	0.060	0.069
Gender	0.498***	0.158	-0.165	-0.167	-0.035	-0.143	-0.041
Information Sensitivity	0.044	-0.177	-0.027	0.138	0.169	0.065	-0.038
Targeted Ads	0.073	0.161	0.079	-0.307*	-0.152	-0.165	-0.205

Statistical significance levels are indicated as: (*) for $p < .05$, (**) for $p < .01$, (***) for $p < .001$.

Table 6: Significant regression co-efficient values for privacy behavior measured against the six EFA factors as dependent variables for Saudi respondents.

Factors	Blocking	Auto Download	Location	Notification	Profile Photo	Last Seen	Status
Intercept	1.292***	-0.384*	1.244***	2.303***			
Sensitive Data	-0.159	0.194	0.082	-0.452	0.152	-0.016	-0.096
Usage Platform	-0.164	0.031	-0.056	-0.169	0.353*	0.018	0.253
Usage Frequency	-0.153	0.079	0.254	0.006	-0.098	-0.038	-0.032
Education and Group Permission	-0.141	-0.017	0.051	0.0368	0.304	0.320*	0.215
Age and Targeted Ads	0.101	0.170	-0.267	-0.168	0.169	0.025	0.084
Professional Contact	-0.438	0.356*	-0.043	0.421*	0.081	0.184	-0.137

Statistical significance levels are indicated as: (*) for $p < .05$, (**) for $p < .01$, (***) for $p < .001$.

Table 7: Significant regression co-efficient values for privacy behavior measured against the six EFA factors as dependent variables for Indian respondents.

channels if they happen to be in a common group. While the current version of WhatsApp asks the user if they want to receive communication from someone not in their contact list, it does not prevent strangers from reaching users over other communication channels like text messages or phone calls.

A way to enforce this would be to replace contact information sharing with username (or similar) sharing. This would protect both users who are stranger-averse and those being cyber-bullied. A way to ensure advanced permission-based contact would be to allow a mechanism for **cooperative blocking**. Due to the nature of WhatsApp as a messaging platform, there is not a centralized way to report platform abuse. Blocking is limited to individuals even though WhatsApp is used as a social platform with large groups. Allowing communities to self-organize and block individuals collectively would enhance the usability of the platform and the autonomy of users. This is also a practice that can be extended to messaging applications which do not have a permission-based contact mechanism in place.

5.2 Choice and Consent in Joining Groups

Respondents from both the samples in our dataset wanted to be asked before being added to a group. Given that users restricted content and access based on group permissions, it is likely that this is more than a social construct and privacy controls that allow users the ability to consent before being added to a group must exist. Messaging applications at large would benefit from this consent process as group communication become increasingly prevalent.

5.3 Option for Group Types

Saudi users seemed to use WhatsApp in a more personal setting given that being contacted by colleagues was not significantly higher. On the other hand, WhatsApp is frequently used in India for contacting colleagues in workplaces and other professional contacts. Our findings indicate that privacy behavior on WhatsApp was effected by user choice to interact with professional contacts. This is possibly because users have different self-presentation for their personal and professional lives [51]. Our findings amplify previous research on WhatsApp as well where qualitative research has stressed the importance of "communication places" to separate group interaction over WhatsApp [45].

Enabling easy *segregation of users into high level groups such as work and family* and having audience based information boundaries would ensure that users are able to share selectively without worrying about boundary management between close members and co-workers (especially with more broadcast features like *Live Status*). Such group-based access control can be applied to other messaging applications as well.

While the above design implications are yet to be tested, they extend directly from our findings and serve as some of the

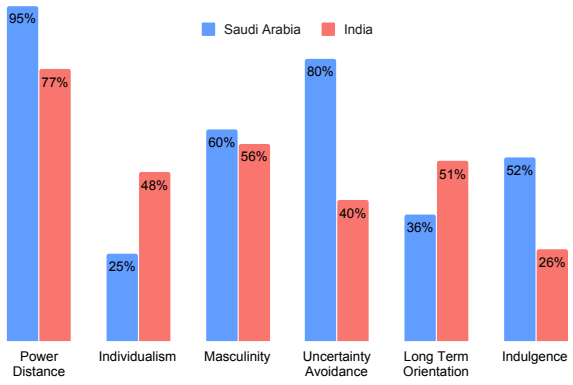
possibilities to make WhatsApp (and possibly other similar messaging applications) more privacy-sensitive and to cater to complex privacy expectations, enhance risk communication and improve trust. Privacy behavior variables like *Blocking*, *Auto Download*, *Location*, *Notification*, *Profile Photo*, *Last Seen*, and *Status* are present in other messaging platforms like Facebook Messenger and Signal as well, and can be similarly studied to view the effect of privacy concerns over behavior.

Though measuring the different dimensions of culture elaborated in Hofstede's work is not covered in the breadth of this study, the influence of nationality seems to hint at the underlying cultural values that affect both privacy concerns and privacy behavior. Figure 5 shows the Hofstede's cultural values measured in terms of power distance, individualism, masculinity, uncertainty avoidance, long term orientation, and indulgence [27] (adopted from Hofstede Insights [30]). Some of these factors may help explain the privacy behavior that we observed in our study. For example, the greater likelihood of Saudis to avoid uncertainty in social situations might drive their reluctance to interact with strangers. Similarly, higher sense of individualism among Indians might explain why they did not want to be contacted by colleagues beyond their workplace. However, these are only conjectures and a future study could help explain the same.

6 Conclusion

Our findings indicate that privacy concerns had both similarities and differences between Saudi and Indian users, both of which were non-WEIRD populations. These privacy concerns combined with demographics like gender affected the privacy behavior of users on WhatsApp in very specific and distinct ways.

Figure 5: Hofstede's cultural dimensions in Saudi Arabia and India (estimates).



Privacy behavior had differences between populations. However, there were also similarities. This allows an opportunity for mobile messaging platforms to enforce both universal and culture-specific boundary management. Privacy behavior was also socially situated, with Indian participants most likely to hide change feature settings to restrict content from professional contacts rather than friends or family. **Most participants in both populations wanted to be able to control the content and recipient (with a greater focus on recipients) of their shared information**.

A core observation, and one which calls for more research is that WhatsApp is experienced as a social network application rather than a messaging application. The embedded use of large groups and workplace-linked contact norms indicate that user perception of WhatsApp is very socially grounded. This leaves an opportunity for a more nuanced re-examination of how privacy settings are implemented. However, our findings cannot be generalized across all non-western populations. A more large scale study with different nationalities across different messaging platforms would be a richer description of privacy concerns in mobile applications. Nevertheless, the results serve to inform the importance of inclusiveness in design choices for privacy–impinging technologies that reach across the globe.

We hope that a brief comparative study would highlight some of the more culturally and socially grounded privacy choices that non-WEIRD populations make. An in-depth cultural study would add to the findings in explaining the norms behind why these privacy choices come into practice in such populations. Religion, political climate, economic models, personal freedom, and societal norms among many others could influence the way people interact with others on mobile messaging platforms, of which WhatsApp is a widely used example.

We used datasets from two populations available to us in order to study cross-cultural privacy concerns and behavior. Studies which include participants from multiple countries, would inform a richer perspective on how different cultures value privacy. In addition, studying the different cultural aspects of privacy might be useful not only to make messaging platforms like WhatsApp sensitive to privacy preferences but also identify areas where cultures reconcile, and create a shared notion of privacy defaults. As mobile messaging platforms increase, largely due to low data usage in non-WEIRD countries, future studies could address different aspects of lesser studied populations to informa privacy choices.

Another aspect that would benefit from follow-up research would be the effect of technical expertise on privacy choices in non-WEIRD populations. Technical expertise [20, 56] and innate privacy sensitivity [37, 41] have long been hypothesized as a measure of privacy behavior and could be implemented in future work.

Acknowledgments

We would like to thank Sanchari Das and Yasmeen Rashidi for their valuable support in implementation of the surveys and data collection. This research was supported in part by the National Science Foundation under CNS 1565375.

References

[1] Norah Abokhodair and Sarah Vieweg. Privacy & Social Media in the Context of the Arab Gulf. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*, pages 672–683, 2016.

[2] Alessandro Acquisti and Ralph Gross. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In *International Workshop on Privacy Enhancing Technologies*, pages 36–58. Springer, 2006.

[3] Andrew A Adams, Kiyoshi Murata, and Yohko Orito. The Japanese Sense of Information Privacy. *AI & society*, 24(4):327–341, 2009.

[4] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. 2017.

[5] Madawi Al-Rasheed. *A Most Masculine State: Gender, Politics and Religion in Saudi Arabia*. Number 43. Cambridge University Press, 2013.

[6] Anita L Allen and Erin Mack. How Privacy Got its Gender. *N. Ill. UL Rev.*, 10:441, 1989.

[7] Irwin Altman. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of social issues*, 33(3):66–84, 1977.

[8] Ann Bartow. Our Date, Ourselves: Privacy, Propertization, and Gender. *USFL Rev.*, 34:633, 1999.

[9] Ulrich Beck and Cordula Kropp. Environmental Risks and Public Perceptions. In *Handbook on Environment and Society*, chapter 41, pages 1205–1216. Sage, 2007.

[10] 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.

[11] Susan Bennett et al. GDPR: Change to European Privacy Laws and its Impact on Australian Businesses. *Governance Directions*, 70(2):85, 2018.

[12] Victor S. Bursztyn and Larry Birnbaum. Thousands of Small, Constant Rallies: A Large-Scale Analysis of Partisan WhatsApp Groups. In *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, ASONAM '19, page 484–488, New York, NY, USA, 2019. Association for Computing Machinery.

[13] Josemar Alves Caetano, Gabriel Magno, Marcos Gonçalves, Jussara Almeida, Humberto T. Marques-Neto, and Virgílio Almeida. Characterizing Attention Cascades in WhatsApp Groups. In *Proceedings of the 10th ACM Conference on Web Science*, WebSci '19, page 27–36, New York, NY, USA, 2019. Association for Computing Machinery.

[14] Karen Church and Rodrigo de Oliveira. What's Up with Whatsapp? Comparing Mobile Instant Messaging Behaviors with Traditional SMS. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, MobileHCI '13, page 352–361, New York, NY, USA, 2013. Association for Computing Machinery.

[15] Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location Disclosure to Social Relations: Why, When, & What People Want to Share. In *SIGCHI Conference on Human Factors in Computing Systems*, pages 81–90. ACM, 2005.

[16] Marc Cornock. General Data Protection Regulations (GDPR) and Implications for Research. *Maturitas*, 111:A1 – A2, 2018.

[17] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. A Study on the Value of Location Privacy. In *Workshop on Privacy in Electronic Society*, pages 109–118. ACM, 2006.

[18] Jayati Dev, Sanchari Das, and L Jean Camp. Poster: Understanding Privacy Concerns of WhatsApp Users in India. In *Symposium and Bootcamp on Hot Topics in the Science of Security*, page 28. ACM, 2018.

[19] Jayati Dev, Sanchari Das, and L Jean Camp. Privacy Practices, Preferences, and Compunctions: WhatsApp Users in India. In *International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, page 135, 2018.

[20] Serge Egelman and Eyal Peer. Predicting Privacy and Security Attitudes. *SIGCAS Comput. Soc.*, 45(1):22–28, February 2015.

[21] Vaibhav Garg, Kevin Benton, and L Jean Camp. The Privacy Paradox: a Facebook Case Study. In *2014 TPRC conference paper*, 2014.

[22] Vaibhav Garg and L Camp. Ex Ante vs Ex Post: Economically Efficient Sanctioning Regimes for Online Risks. *Research Conference on Communication, Information and Internet Policy*, 2013.

[23] David A Grimes and Kenneth F Schulz. Making Sense of Odds and Odds Ratios. *Obstetrics & Gynecology*, 111(2):423–426, 2008.

[24] Swati Gupta and Bard Wilkinson. WhatsApp India: Five Lynched after Online Child Kidnap Rumors. https://www.cnn.com/2018/07/02/asia/india-lynching-whatsapp-intl/index.html, July 2018. (Accessed on 02/15/2019).

[25] Joseph Henrich, Steven J Heine, and Ara Norenzayan. Most People are not WEIRD. *Nature*, 466(7302):29, 2010.

[26] Brent Dale Hill. *Sequential Kaiser-meyer-olkin Procedure as an Alternative for Determining the Number of Factors in Common-factor Analysis: a Monte Carlo Simulation*. PhD thesis, Oklahoma State University, 2011.

[27] Geert Hofstede. Cultural Dimensions. *LIUC (IT)*, 13, 2003.

[28] Mariea Grubbs Hoy and George Milne. Gender Differences in Privacy-Related Measures for Young Adult Facebook Users. *Journal of Interactive Advertising*, 10(2):28–45, 2010.

[29] Christopher Hsee and Elke U Weber. Cross-cultural Differences in Risk Perception, but Cross-Cultural Similarities in Attitudes Towards Perceived Risk. *Management Science*, 44(9):1205, 1998.

[30] Hofstede Insights. Cross-Country Comparison. https://www.hofstede-insights.com/country-comparison/, April 2020. (Accessed on 04/02/2020).

[31] Henry F Kaiser. The Application of Electronic Computers to Factor Analysis. *Educational and Psychological Measurement*, 20(1):141–151, 1960.

[32] Naz Kaya and Margaret J Weber. Cross-cultural Differences in the Perception of Crowding and Privacy Regulation: American and Turkish Students. *Journal of environmental psychology*, 23(3):301–309, 2003.

[33] Simon Kemp. Saudi Arabia Social Media Statistics 2018. https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/, January 2018. (Accessed on 02/15/2019).

[34] Jennifer King, Airi Lampinen, and Alex Smolen. Privacy: Is There an App for That? In *Symposium on Usable Privacy and Security*, page 12. ACM, 2011.

[35] Paul Kline. *An Easy Guide to Factor Analysis*. Routledge, 2014.

[36] Alfred Kobsa, Sameer Patil, and Bertolt Meyer. Privacy in Instant Messaging: An Impression Management Model. *Behaviour & Information Technology*, 31(4):355–370, 2012.

[37] Ponnurangam Kumaraguru and Lorrie Faith Cranor. Privacy Indexes: A Survey of Westin's Studies. *Carnegie Mellon University*, 2005.

[38] Rebecca K Lee. Romantic and Electronic Stalking in a College Context. *Wm. & Mary J. Women & L.*, 4:373, 1997.

[39] Kevin Lewis, Jason Kaufman, and Nicholas Christakis. The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer-Mediated Communication*, 14(1):79–100, 2008.

[40] Yao Li, Alfred Kobsa, Bart P Knijnenburg, and MH Carolyn Nguyen. Cross-cultural Privacy Prediction. *Proceedings on Privacy Enhancing Technologies*, 2017(2):113–132, 2017.

[41] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4):336–355, 2004.

[42] Sara Malm. Saudi Arabian Man gets 40 Lashes for Insulting ex-Wife on WhatsApp. https://www.dailymail.co.uk/news/article-6388353/Saudi-Arabian-man-gets-40-lashes-insulting\/-ex-wife-WhatsApp.html, November 2018. (Accessed on 02/15/2019).

[43] Patrick E McKnight and Julius Najab. Mann-Whitney U Test. *The Corsini Encyclopedia of Psychology*, pages 1–1, 2010.

[44] Patricia Brierley Newell. A Cross-cultural Comparison of Privacy Definitions and Functions: A Systems Approach. *Journal of Environmental psychology*, 18(4):357–371, 1998.

[45] Midas Nouwens, Carla F. Griggio, and Wendy E. Mackay. "WhatsApp is for Family; Messenger is for Friends": Communication Places in App Ecosystems. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, page 727–735, New York, NY, USA, 2017. Association for Computing Machinery.

[46] Times of India. WhatsApp to Cap Message Forwarding to 5 Chats Globally. https://timesofindia.indiatimes.com/business/india-business/whatsapp-to-cap-message-forwarding-to-5-\/chats-globally/articleshow/67623233.cms, January 2019. (Accessed on 01/25/2019).

[47] Department of Justice. Privacy Act of 1974, 1974.

[48] Daniela Seabra Oliveira, Jeremy Epstein, James Kurose, and Anderson Rocha. Cybersecurity and Privacy Issues in Brazil: Back, Now, and Then [Guest Editors' Introduction]. *IEEE Security & Privacy*, 16(6):10–12, 2018.

[49] Kenton P. O'Hara, Michael Massimi, Richard Harper, Simon Rubens, and Jessica Morris. Everyday Dwelling with WhatsApp. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work Social Computing*, CSCW '14, page 1131–1143, New York, NY, USA, 2014. Association for Computing Machinery.

[50] Sameer Patil and Alfred Kobsa. Instant Messaging and Privacy. In *Human-Computer Interaction*, volume 4, pages 85–88, 2004.

[51] Sameer Patil, Alfred Kobsa, Ajita John, and Doree Seligmann. Comparing Privacy Attitudes of Knowledge Workers in the US and India. In *International Conference on Intercultural Collaboration*, pages 141–150. ACM, 2010.

[52] Iryna Pentina, Lixuan Zhang, Hatem Bata, and Ying Chen. Exploring Privacy Paradox in Information-sensitive Mobile App Adoption: A Cross-cultural Comparison. *Computers in Human Behavior*, 65:409–419, 2016.

[53] Sankalp Phartiyal and Aditya Kalra. Indian Political Parties Abuse WhatsApp Service Ahead of Elections. https://www.reuters.com/article/us-india-whatsapp/indian-political-parties-abuse-whatsapp-\/service-ahead-of-election-executive-\/idUSKCN1PV1E3, February 2019. (Accessed on 02/15/2019).

[54] Bandana Purkayastha, Mangala Subramaniam, Manisha Desai, and Sunita Bose. The Study of Gender in India: A Partial Review. *Gender & Society*, 17(4):503–524, 2003.

[55] Prashanth Rajivan and Jean Camp. Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices. In *Authentication Workshop of the 12th Symposium on Usable Privacy and Security*. USENIX Association, 2016.

[56] Prashanth Rajivan, Pablo Moriano, Timothy Kelley, and L Jean Camp. Factors in an End-user Security Expertise Instrument. *Information & Computer Security*, 25(2):190–205, 2017.

[57] Yasmeen Rashidi, Kami Vaniea, and L Jean Camp. Understanding Saudis Privacy Concerns when using WhatsApp. In *Workshop on Usable Security (USEC)*, 2016.

[58] Gustavo Resende, Johnnatan Messias, Márcio Silva, Jussara Almeida, Marisa Vasconcelos, and Fabrício Benevenuto. A System for Monitoring Public Political Groups in WhatsApp. In *Proceedings of the 24th Brazilian Symposium on Multimedia and the Web*, WebMedia '18, page 387–390, New York, NY, USA, 2018. Association for Computing Machinery.

[59] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for Me, it's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 127–142, 2018.

[60] Balla Satish. How WhatsApp Helped Turn an Indian Village into a Lynch Mob. https://www.bbc.com/news/world-asia-india-44856910, July 2018. (Accessed on 02/15/2019).

[61] Paul Sawers. Why WhatsApp Scrapped Its $1 Annual Subscription Fee. https://venturebeat.com/2016/01/18/whatsapp-subscription/, January 2016. (Accessed on 05/26/2020).

[62] Manish Singh. WhatsApp Hits 200 Million Active Users in India. http://mashable.com/2017/02/24/whatsapp-india-200-million-active-users/#Dka5Ao6c5sqW, February 2017. (Accessed on 05/26/2020).

[63] Statista. WhatsApp: Mobile Usage Penetration by Country. https://www.statista.com/statistics/291540/mobile-internet-user-whatsapp/. (Accessed on 02/23/2020).

[64] Ryan Theodosia. Being (Nonbinary) Transgender in a Census Year, May 2019.

[65] MS Thirumalai and B Mallikarjun. The Official Language Act, 1963 (As Amended, 1967). *Language in India: Strength for Today and Bright Hope for Tomorrow*, 2002.

[66] Sigmund Tobias and James E Carlson. Brief Report: Bartlett's Test of Sphericity and Chance Findings in Factor Analysis. *Multivariate Behavioral Research*, 4(3):375–377, 1969.

[67] Blase Ur and Yang Wang. A Cross-cultural Framework for Protecting User Privacy in Online Social Media. In *Proceedings of the 22nd International Conference on World Wide Web*, pages 755–762. ACM, 2013.

[68] Paul van Schaik, Jurjen Jansen, Joseph Onibokun, Jean Camp, and Petko Kusev. Security and Privacy in Online Social Networking: Risk Perceptions and Precautionary Behaviour. *Computers in Human Behavior*, 78:283–297, 2018.

[69] Yang Wang, Gregory Norice, and Lorrie Faith Cranor. 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*, pages 146–153. Springer, 2011.

[70] Alan F Westin. Privacy and Freedom. *Washington and Lee Law Review*, 25(1):166, 1968.

[71] K Yoshida. Performing Multiple t-tests on Different Variables Between the Same Two Groups. 2013.

[72] Seounmi Youn and Kimberly Hall. Gender and Online Privacy Among Teens: Risk Perception, Privacy Concerns, and Protection Behaviors. *Cyberpsychology & behavior*, 11(6):763–765, 2008.

[73] Norhayati Zakaria, Jeffrey M Stanton, and Shreya TM Sarkar-Barney. Designing and Implementing Culturally-sensitive IT Applications: The Interaction of Culture Values and Privacy Issues in the Middle East. *Information Technology & People*, 16(1):49–75, 2003.

A Appendix: Survey Instrument (Excerpt) and Table of Variables

Please note that the numbers are for ordering the options, and are not necessarily used in the same order for the analysis

- What is your age?
  (1) Less than 18 years (2) 18-24 years (3) 25-30 years (4) 31-40 years (5) 41-50 years (6) More than 50 years
- Do you have a WhatsApp account?
  (1) Yes (2) No
- Which operating system do you currently use for your primary smartphone?
  (1) Android (2) iOS (3) Windows (4) Blackberry (5) Symbian (6) Other. Specify.
- Are you concerned that since Facebook bought WhatsApp, targeted ads might start appearing in WhatsApp?
  (1) Definitely yes (2) Probably yes (3) Might or might not (4) Probably not (5) Definitely not
- How long have you been using WhatsApp?
  (1) Less than 1 year (2) 1-2 years (3) 2-3 years (4) 3-4 years (5) 4-5 years (6) More than 5 years
- Do you use the latest updated version of WhatsApp?
  (1) Yes (2) No (3) I don't know
- On average, how often do you use WhatsApp?
  (1) More than once a day (2) Daily (3) More than once a week (4) Once a week (5) More than once a month (6) Once a month (7) More than once a year (8) Once a year (9) Never
- Auto-download feature in WhatsApp allow your media (e.g. images, audio, and video) to be downloaded automatically without the need to explicitly do it manually. This feature is automatically activated in WhatsApp which can be altered later by going to the WhatsApp settings. Did you disable the auto-download feature on WhatsApp?
  (1) Yes (2) Maybe (3) No (4) I do not know
- Blocked feature in WhatsApp allows its users to add any person to the blocked list to prevent them from contacting the user. Did you use the Blocked feature in WhatsApp to block any person from contacting with you?
  (1) Yes (2) Maybe (3) No (4) I do know about this feature
- Have you enabled WhatsApp to send you notifications when there is a new message?
  (1) Yes (2) No (3) I do not know
- Have you previously shared your location using WhatsApp?
  (1) Yes (2) No (3) I did not know about the feature
- I frequently use WhatsApp to send/share private or sensitive chats/media:
  (1) Strongly agree (2) Somewhat agree (3) Neither agree nor disagree (4) Somewhat disagree (5) Strongly disagree
- Are you concerned that anyone who has your phone number is able to contact you and see the activity shared publicly using WhatsApp?
  (1) Yes (2) Maybe (3) No (4) I do not care
- When adding me to a group chat, I would like the app to:
  (1) Definitely ask me before adding (2) Ask me before adding only to specific groups (3) Does not really need to ask me before adding (4) I don't care
- WhatsApp has some privacy features. It allows you to show your last seen, profile photo or/and status to everyone (default option), just the people on your contact list, selectively choose some people, or nobody. What is your setting in each of the following: [Everyone (1) My Contacts (2) Nobody (3) I do not know (4)] (1) Last Seen (2) Profile Photo (3) Status (4) Live Location (5) Read Receipts

Research Questions	Independent Variables	Dependent Variables
RQ1, RQ2 (MWW Test)	(1) Origin/ Nationality (2) Gender	(1) Sensitive Data (2) Professional Contact (3) Targeted Ads (4) Group Add Ask (5) Stranger Contact Concern
RQ3 (Exploratory Factor Analysis)	(1) Sensitive Data (2) Professional Contact (3) Targeted Ads (4) Group Add Ask (5) Stranger Contact Concern (6) Platform (7) Frequency (8) Length (9) Age (10) Gender (11) Education	**Saudi** (1) Sensitive Data (2) Usage Platform (3) Usage Frequency (4) Education and Group Permission (5) Age and Targeted Ads (6) Professional Contact **India** (1) Age and Education (2) Usage Platform (3) Gender (4) Information Sensitivity (5) Targeted Ads
RQ3 (Regression Analysis)	**Saudi** (1) Sensitive Data (2) Usage Platform (3) Usage Frequency (4) Education and Group Permission (5) Age and Targeted Ads (6) Professional Contact **India** (1) Age and Education (2) Usage Platform (3) Gender (4) Information Sensitivity (5) Targeted Ads	(1) Blocking (2) Auto Download (3) Location (4) Notification (5) Profile Photo (6) Last Seen (7) Status

Table 8: List of independent and dependent variables for each research questions.

- What is your primary country of citizenship?
- Which gender do you identify with the most? (1) Female (2) Male (3) Other (4) Do not wish to specify
- What is the highest level of education you have completed? (If currently enrolled, highest degree received.) (1) Less than high school (2) High school graduate (3) Diploma (4) Vocational training (5) Bachelors degree program (6) Masters degree program (7) Professional degree (8) Doctorate (9) Other. Specify.