What about my Privacy, Habibi?

Understanding Privacy Concerns and Perceptions of Users from Different Socioeconomic Groups in the Arab World

Mennatallah Saleh[1,2], Mohamed Khamis[3], and Christian Sturm[1]

[1] Hamm-Lippstadt University of Applied Science, Germany
[2] Technical University of Berlin, Germany
[3] University of Glasgow, Glasgow, UK
Menna.eSaleh@gmail.com, Mohamed.Khamis@glasgow.ac.uk,
Christian.Sturm@hshl.de

Abstract. This paper contributes an in-depth understanding of privacy concerns and perceptions of Arab users. We report on the first comparison of privacy perceptions among 1) users from high socioeconomic groups in Arab countries (HSA), 2) users from medium to low socioeconomic groups in Arab countries (LSA), and 3) as a baseline, users from high socioeconomic groups in Germany (HSG). Our work is motivated by the fact that most research in privacy focused on Western, Educated, Industrialized, Rich, and Democratic (WEIRD) societies. This excludes a segment of the population whose cultural norms and socioeconomic status influence privacy perception and needs. We report on multiple novel findings and unexpected similarities and differences across the user groups. For example, shoulder surfing is more common across LSA and HSG, and defamation is a major threat in LSA. We discuss the implications of our findings on the design of privacy protection measures for investigated groups.

Keywords: Emerging users · privacy · culture · WEIRD · Arabs

1 Introduction

The ubiquity of technology around us has brought users a myriad of benefits. On the downside, the ability to access private information almost anywhere and at anytime comes with implications on user privacy. Acknowledging this issue, a plethora of research investigated the privacy perceptions and concerns of users [18, 21, 34, 35, 39, 54]. While these works significantly extended our understanding of user privacy, it remains unclear if these findings generalize to the wider populations of the world. In particular, there is a gap in the knowledge of privacy perceptions and concerns of Arab users and the societies within the Arab world.

This problem is amplified by the fact that the vast majority of previous studies in this area were conducted with participants from Western, Industrialized, Rich, and Democratic (WEIRD) societies [36, 37]. The term WEIRD was coined by Henrich et al. [37] in 2010, and since then researchers in behavioral psychology have acknowledged that participants from WEIRD societies can often be

psychological outliers [36, 37] because they represent less than 15% of the world population. The Human-Computer Interaction community has recently acknowledged this issue in HCI research too [60]. Furthermore, there has been a recent increasing interest within the Usable Security and Privacy community to move away from "one-size fits all" approach [66]. Since socioeconomic groups and cultures are known to influence users' perceptions of technology and its implications [15, 42, 44], it is important to consider the potential impact of the socioeconomic profile on the individual's privacy perceptions. For example, would sharing of a mobile device be perceived to out-weigh privacy concerns for low-income individuals? Do Arabs' emphasis on reputation influence their protective measures against privacy invasion? These reasons underline the necessity to expand our understanding of privacy needs and concerns of different user groups, including users from different cultures, as well as users from different socioeconomic groups. To contribute in this direction, we focus on different socioeconomic groups within the Arab world, and compare results to participants from WEIRD societies.

We chose the context of Arabs since their privacy needs and concerns are relatively under-investigated in the literature. We expect to find novel concerns and perceptions among this user group due to the unique cultures and values that are shared among Arab countries. Preliminary investigations have already suggested that there may be significant differences in privacy invasion experiences between Arabs and non-Arabs [54]. To name a few relevant examples: Arabs adhere to cultural values that could influence privacy perceptions. This, in turn, could have an impact on the perceived implications of privacy violations. For example, Arab women who wear a headscarf, aka Hijab, are likely to be more careful in protecting their private pictures from men who are not part of the woman's family. They could, in turn, perceive the leak of private pictures to be more dangerous compared to women in other societies. Another example is the significance of dignity and reputation in the Arab world [59, 61]; an ill-reputation caused by acts of defamation could influence an Arab's relationships, as well as social and economic opportunities. These differences encouraged the CHI, DIS and CSCW communities to investigate needs and concerns of Arab users in the respective fields [5, 8, 41, 51, 62].

In this work, we report on the first in-depth investigation of privacy concerns and perceptions of users from high and medium to low socioeconomic groups in two Arab countries. We refer to them hereafter as **HSA** and **LSA** for short. We limited our pool of participants to those who are residing in said countries to reduce the influence of external factors. As a baseline for comparison, we compare results to participants from high socioeconomic groups in Germany (**HSG**). In particular, we report on a survey (N=156) that was distributed among participants who are from and reside in Egypt, Saudi Arabia, and Germany. We reached out for HSA and HSG participants through a questionnaire distributed online, and LSA participants by distributing a printed Arabic translation of the questionnaire to workers of a hospital. Among the findings, we found that consequences of privacy invasion could be particularly severe for LSA users, and

that shoulder surfing occurs more often among LSA and HSG participants. We discuss the implications on designing privacy protection for said communities.

2 Related Work

In 1986, Shwartz discussed the phenomenon of withdrawal into privacy. He showed how increasing the secrecy and boundaries between people causes more intrigue and hence makes these boundaries more likely to be broken by others [58]. However, with the widespread use of social networks, some argue that social norms evolved and users are now comfortable sharing information openly with others [67]. We investigate the current state of privacy concerns and perceptions in low and high socioeconomic Arab groups.

2.1 Studying Privacy Perceptions

Privacy invasion has been studied in multiple situations. Types of privacy invasion attacks that were investigated include identity theft, impersonation, spying, profile harvesting, defamation, impersonation, credit card theft and shoulder surfing [23, 40]. Shoulder surfing is defined as the act of observing other peoples information without their consent [23].

Every society values and expresses privacy differently than others [65]. The concept of the "average user" is now being abolished by many researchers. Egelman and Peer introduced psychographic targeting of privacy and security mitigations that relied on user profile understanding [22]. They found that decision making styles were better predictors for privacy attitudes than the Big Five personality traits. Wisniewskia et al. also categorized users into six profiles depending on their sharing and privacy attitudes on Online Social Networks (OSNs) and offered design implications for each user group [68]. Yoo et al. investigated the effect of the hacking of a popular online Korean market on the privacy perceptions of its users [70]. Findings show that mild previous experiences reduce the perceptions of loss and that privacy concerns increase loss perceptions.

This suggests that privacy perception is influenced by one's background. Next, we discuss how cultural backgrounds influence privacy perceptions.

2.2 Cultures and Privacy Interplay

Sambasivan et al. emphasized the importance of understanding the role culture plays in technology use and hence its influence on design [56].

Cultures also play a central role in shaping privacy concerns and perceptions. Privacy researchers also noticed this gap and attempted to investigate influences of national culture on privacy perception. Dinev et al. compared privacy perception about government surveillance in USA and Italy [18]. Results show that Italian participants had lower privacy concerns. Habrach et al. conducted a survey on eight countries concluding that Japanese and German participants had higher privacy concerns on their smartphones than those from Australia,

Canada, Italy, Netherlands, UK and USA. A survey on 325 Arab participants showed that females are more concerned than males about their online privacy and that Egyptians are more comfortable with privacy on social networks than Emiratis [48]. Li et al. have predicted privacy based on the cultural dimensions of an individual, emphasizing the importance of the difference culture makes in privacy decision making [44]. Harbach et al. compared risk perceptions across USA and Germany [34]. They found that participants from USA were more concerned about identity theft, while Germans were more concerned about hidden costs in services, frauds and scams. Eiband et al. collected real shoulder surfing stories from participants from different countries including Germany, Egypt, USA, Bulgaria, India, Italy, Romania, Russia and South Korea [23]. However their aim was not to compare cultures, bur rather to find evidence for shoulder surfing in the real world; they did confirm that it is a real threat that indeed occurs and has negative consequences on the user. Bellman et al. investigated how the Hofstede cultural dimensions affect the perception and found that individualism, masculinity and power distance all affected privacy attitude [13].

While national culture is a very important predictor of privacy perceptions and attitudes, it is not sufficient. Wang et al. show the important role education plays in privacy and how the participants with higher education have higher privacy concerns [63]. Schwartz labels privacy as a luxury that not all users can afford [58], and some users seem to agree [55]. Other researchers noticed phenomena such as phone sharing and designed solutions that increase security for these setups [53]. These works suggest that socioeconomic factors, such as education and income, also influence privacy perceptions. There is a need to revisit the claim of privacy affordability due to the myriad of sensitive information that is at risk of privacy invasion, and due to its potential serious consequences particularly in underdeveloped and conservative cultures. Acknowledging this, some researchers investigated ways of improving security for emergent users [38]. For example, previous work looked into increasing security in phone sharing scenarios among emergent users [53, 3]. Ahmed et al. studied privacy invasions by local repair shops in Bangladesh [2]. They found that repairers often look at private contents on customers' phones. In another study, Ahmed et al. studied how government-imposed mandatory biometric registration for each mobile phone results in concerns and suspicions within the Bangladeshi population [4]. Sambasivan et al. studied how women in south Asia navigate privacy within complicated gender power balance [55].

These works underline the importance of understanding the influence of both geographic and socioeconomic distributions on privacy perceptions.

3 Target Groups

Previous work in privacy and security reveals that there is a gap in understanding the privacy concerns and perceptions of users from the Arab world. Furthermore, there has been a steadily increasing adoption of technology among more users

of low socioeconomic groups, This user group shows a set of under-investigated design needs and concerns that are influenced by their unique privacy perception.

Preliminary work in this area has shown that there might be significant differences in privacy invasion experiences in Arab communities compared to non-Arab ones [54]. It has also been established that a person's level of income could influence their privacy concerns [58]. This led us to add two target groups in our work: Users from **H**igh **S**ocioeconomic groups in **A**rab countries (HSA), and users from **L**ow **S**ocioeconomic groups in **A**rab countries (LSA). We chose to study two Arab countries: Egypt and Saudi Arabia. Egypt is the Arab country in Africa with the most internet users (over 37 million users), Saudi Arabia the Arab country in the Middle East with the most internet users (24 million out of a 32 million population) [31]. Egypt and Saudi Arabia are Arab countries that share many cultural dimensions due to common traditions and religion [30, 26].

Second, we chose users from **H**igh **S**ocioeconomic groups in **G**ermany (HSG) as a baseline because (1) it is a typical Western, Educated, Industrialized, Rich and Democratic society, (2) this user group has been extensively studied in previous work [23, 33–35]. We focused our work on women because previous work has shown that women have more privacy concerns in the Arab world, so we recruited more female participants [12, 1].

4 Questionnaire Development

The questionnaire[4] was distributed online to high socioeconomic participants (HSA and HSG) and offline for medium to low socioeconomic participants (LSA). The questionnaire was developed in English and translated to Arabic for LSA participants. Its translation was validated in terms of language and cultural appropriateness by native speakers. A challenge in cultural studies in HCI is ensuring that questions are tapping into the same constructs when the questionnaire is administered in different cultures [16]. Thus, to ensure cultural appropriateness, we conducted a pre-study where participants were asked to answer the questionnaire then explain any difficulties or comments. Participants had some issues with the questionnaire structure which we edited, but there were no cultural issues reported. In addition, we are also familiar with the cultural backgrounds of all our user groups by being integrated in their communities. We used non-biased wordings and provided more space for participants to use their own words through critical incident recall and open ended questions.

4.1 Questionnaire Design

National culture was determined by asking participants where they are from and where they reside. Socioeconomic status was determined through anonymous questions about the participant's occupation, income, education, and residence type, which are the most widely recognized measures for determining socioeconomic statuses [28, 25]. The questionnaire was designed to collect very sensitive

[4] Questionnaire can be found in the supplementary material section on Springer

data, so the anonymity of the results and its separation from the demographic data was emphasized throughout the questionnaire. This has been shown to ensure high level of honesty when answering questions [45].

We used the critical incident technique [9]. Participants were asked to freely recall a privacy violation incident using critical incidents that they have experienced or have witnessed. This facilitates the narration of the experiences and makes the reflection on the questions more reliable as it relates to own life events. To reduce social desirability bias, no negative connotations were used to describe the attacker or the incidents [20]. Instead, the terms victim and attacker were replaced by gender neutral personas. We used "Vic" and "Cas" in the English version, and "Nour" and "Ehsan" in the Arabic version. We conducted two prestudies with 10 participants in which we iteratively improved the clarity of the questionnaire and its organization by incorporating their feedback. All data was anonymous and that the participants gave an informed consent that we can store and use their anonymous responses for research non-commercial purposes. Participants who filled the online questionnaire and wished to be considered for the shopping voucher provided their emails; we separated emails before analysis and discarded them after compensations were issued. No contact details were collected from those who filled the printed version.

4.2 Questionnaire Structure

The questionnaire was divided into five sections:

Experience with Privacy Invasion The first section collected information about participant's experience with privacy invasion. Several types of privacy invasions were listed and participants were asked to report if they experienced them, and were asked to rank their perceived severity from 1 (Extremely Severe) to 5 (Not Severe at all). Next, participants were asked to report a privacy violation incident they experienced or observed in the form of an open question. This was followed by questions on why participants perceived the situation to involve privacy invasion, and the participant's role in the incident, i.e., whether the participant was Cas, Vic, or a third-party observer.

Details about the Incident In the second section, more information about the privacy invasion incident was collected. We asked for the relationship between the victim and the attacker, the consequences of the attack, the content that was violated, the feelings of the participant towards the incident and the locations and genders of those involved.

Relationships and Privacy Dynamics In the following section, participants were asked to answer when and whom they believe can access their private information without them considering it a privacy violation. Our aim from this question was to understand if participants from the investigated user groups perceive

privacy invasions by certain individuals to be acceptable. This was motivated by preliminary indicators that some Arabs perceive the invasion of children privacy to be justified [54].

Applied Preventative Measures After that, participants were asked to report who they constantly try to protect their information from (e.g., colleagues, family, etc.) and reasons behind that. This was done to investigate if relationships play different roles depending on nationality and/or socioeconomic group.

Demographics and Socioeconomic Group Finally, participants were asked to report their demographics to identify their socioeconomic status, including their occupation, academic degree, residence and monthly income, as well as their country of origin and residence [28, 25]. Inspired by prior work to exclude invalid data [23], we asked participants to rate the honesty of their response on a five-point Likert scale.

4.3 Distribution and Recruitment

In HSA and HSG, due to their educational background they were used to surveys and hence it was easy to introduce ourselves and our survey objectives through mailing lists and social media. For LSA, participants were at first hesitant. We established rapport by visiting the community personally, talking to the participants generally about social media and privacy, and showing them that we are "on their side". The questionnaire was distributed through social networks and through Egyptian, Saudi and German university mailing lists. To include more LSA participants who might not be reachable online, the questionnaire was printed and administered to nurses in 3 hospitals in Egypt. The nurses' educational degrees were either Diplomas or university education with an average salary of less than 3000 EGP per month. Based on their education, occupation and income, they are considered from a medium to low socioeconomic group according to prior work on socioeconomic status scale in Egypt [25]. Participants were compensated with shopping vouchers or credit points for their studies.

4.4 Limitations

Self-report bias is a significant shortcoming of questionnaires [19], and ours it not an exception; participants answer what they thought or believed the situation to be, not what actually happened. We attempted to counteract this by providing neutral connotations for attacker and victim to avoid strong positive or negative associations that would increase the bias. Still, only 12% of participants reported themselves as attackers or "Cas", most likely due to the social desirability bias [20]. Another issue is that to reach out for LSA participants, we administered a paper-based version of the questionnaire. This may have led to bias as online participants are self-selected, i.e., a participant might decide not to fill in the

questionnaire if they do not want to. To balance this potential bias, offline questionnaires that included many empty response fields were excluded completely, and the addition of the honesty question was considered where if participants responded that they were not honest when answering the survey, their result was also excluded. While there are limitations to questionnaires, this tool has given us the ability to reach a wide variety of participants. In addition, using the critical incident recall and allowing participants to use their own words and ideas generated interesting results. We even got feedback from the participants that the questionnaire was intriguing and fun.

5 Results

Table 1 shows a summary of the major results reported by the participants.

The survey was filled by 166 participants. We excluded 8 participants for not answering the majority of questions. Furthermore, we excluded 2 participants who responded "disagree" or "strongly disagree" when asked about the honesty of their responses. Out of the remaining 156 participants, 58 participants were males and 98 were females. The gender bias is due to the LSA group who were mostly female nurses. Out of all participants, there were 39 LSA participants from Egypt, 58 HSA participants (36 from Egypt and 22 from Saudi Arabia) and 61 HSG participants from Germany. Participants' ages ranged from 18 to 57 with a mean age of 31 (SD=10.9).

Responses were coded by one researcher then revised by another to ensure consistency and avoid bias. Open-ended questions were labeled and thematic analysis, loosely based on the work of Guest et al. and Miles et al., was used to extract the following themes [32, 46].

5.1 Theme 1: Experienced Types of Privacy Invasions

In the first section, we asked participants about the types of privacy invasions they experienced. We provided a list of the following privacy invasion attacks, and asked them to choose the ones they have experienced as an attacker, victim or third-party observer. These included identity theft, impersonation, profile harvesting, spying, shoulder surfing, hacking, credit card theft, involuntary attacks. These types of attacks were extracted from [17]; we then added shoulder surfing [23] and credit card theft [40]. Figure 1 shows the type of privacy invasions experienced by all groups.

Results show that while shoulder surfing is the most experienced form of attacks, participants from the HSA do not report it as often. A possible reason is that shoulder surfing occurs mostly in public transport [23] which is commonly used by HSG and LSA, public transport is not commonly used by individuals who belong to high socioeconomic subgroups in the middle east (i.e., HSA participants) [27].

Hacking, identity theft and defamation are generally common, and relatively more common in the LSA group. This is fueled by acts of defamation as a form of vengeance, and the importance of reputation in this culture [29, 52].

Aspect	**LSA**	**HSA**	**HSG**
Hacking	Black Hat	Grey Hat	Grey Hat
Shoulder Surfing	Frequent	Infrequent	Frequent
Perceived Intentions	Malicious and targeted	Random	Random
Consequences of Attack	Serious consequences	Some consequences	No consequences
Acceptability of privacy invasion situations	Not accepted	Accepted in case of parents invading child privacy	In case of death or individual safety
Acceptability of personal information access from individuals	Sometimes by spouses	Sometimes by spouses	Not accepted
Change of privacy perception after an attack	Yes	Yes	No
Most Commonly invaded platforms	smartphones (58.97%)	smartphones (30.19%) and laptops (28.3%)	smartphones (51.79%)

Table 1. Based on the results of a survey (N=156), we report on differences and similarities between users from: Low Socioeconomic Arab societies (LSA), High Socioeconomic Arab Societies (HSA) and High Socioeconomic German Socities (HSG).

According to the Central Bank of Egypt, only 33% of Egyptian adults have bank accounts [49]. Our results show that credit card theft is not experienced often (6 out of 39) among LSA participants since individuals with low income in Arab countries usually do not own credit cards or even bank accounts. On the other hand, it is experienced more often among HSA participants (17 out of 58). It is not often experienced often among HSG (6 out of 61). A possible reason is that Germans tend to prefer cash transactions [11, 34].

Finally, device sharing attacks were only experienced in the LSA group (23 times). This is expected since phone sharing is more common in low socioeconomic societies [69].

In addition to selecting the types of privacy invasions they experienced in the last section, we further asked participants to report a particular privacy invasion

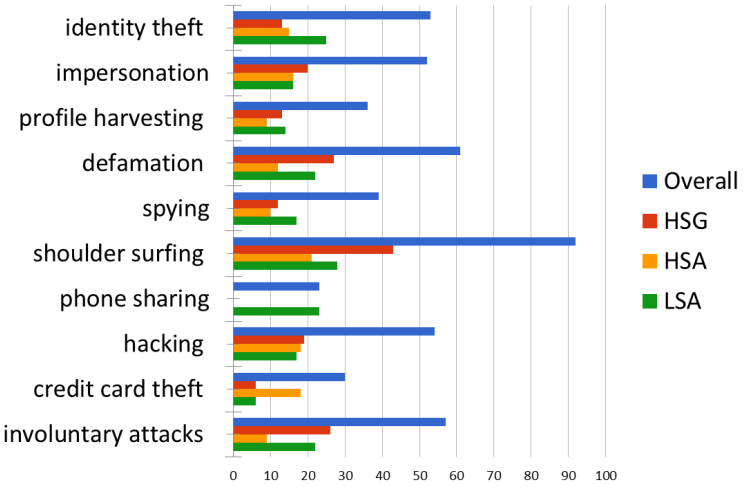

Fig. 1. Number of attacks experienced across the 3 participant groups. The results show that shoulder surfing is one of the most common privacy invasion types experienced across all groups. However, HSG and LSA groups experience it more often than HSA. Credit card theft is less common in HSG and LSA. Identity theft is most common in LSA, while attacks related to device sharing are exclusive to LSAs.

incident that they recall in an open-ended question. We clarified that they can report incidents in which they were attackers, victims, or third-party observers. The following section describes the attack that participants deemed most relevant to report then describe in detail. In addition to the privacy invasions types reported in section 5.1, a new type of privacy invasion emerged from the data, that we labeled "physical breach". We use this term to refer to attacks where the attacker gains access to the victim's device by being physically present in the same place, for example accessing their phone by borrowing it, participants forgetting to logout and attackers using their accounts, or observing the victim's credentials and using them later. We also added a category: "application privacy invasion" as participants complained that applications on their phones invaded their privacy. Most of the LSA (34 out of 39) participants reported forms of hacking as their privacy invasion incidents. This was not matched in HSA (17 out of 58) and HSG (18 out of 61) participants, whose leading form of invasions were physical breach (61 out of 119) and shoulder surfing (45 out of 119).

In addition, LSA participants also reported more "black-hat hacking" cases, i.e., incidents where the hacker has a malicious intent and causes personal damage with actions such as identity theft and defamation. Over 50% (19 out of 34) of the hacking incidents reported by LSA participants involved attackers spreading private information about the victim, in particular personal photos. Personal information was spread to the victim's acquaintances, which often resulted in severe damage to the victim's relationships. One participant walked us through how her relationship with her fiancee was affected after her Facebook profile was

hacked. Over 70% (26 out of 34) of the hacking incidents reported were also directed towards the victim specifically with an intent to personally hurt them and were preempted rather than being random events. Around half (21 out of 34) of these attacks were by strangers, while the other half was by attackers that the victim knew personally, such as colleagues, friends, or sometimes even spouses. This can be due to the revengeful nature of this particular user group [7], this will be discussed in further details in Section 5. In addition, most of the hacking events included female victims (20 out of 37). Many of them included male hackers to female victims (13 out of 37).

On the other hand, most of the attacks experienced by HSA (12 out of 17) and HSG (10 out of 14) were "grey-hat hacking" where the hacker wanted to enjoy the process of hacking and gaining access to the participants account over actually harming them in their personal lives or relationships. Participants from both HSA and HSG groups had their email or Facebook accounts hacked. According to their responses, no real damage occurred with the exception of when hackers requested money from the victim's friends or from the victim himself to recover the account.

5.2 Theme 2: Perceived Intentions of Attackers

Participants were asked about the perceived reasons for the privacy invasion and the intentions of the attacker. In HSA and HSG, responses included coincidence (5), curiosity (14), and boredom (5) which mostly showed mild negative connotation or perception of the attacker. This is also inline with previous findings about certain types of attacks such as shoulder surfing [23]. Some HSA and HSG participants (24 out of 119) reported that the attacker sought money, which showed negative connotation but was not directly related to this particular victim. Participants stated that the attackers who stole the victim's identity asked them or their friends for in return for the account. On the other hand, participants from LSA reported reasons such as revenge, defamation, immoral attacker and spying. This shows that LSA individuals perceive attackers to have a higher negative association than HSA and HSG victims. In addition, LSA individuals reported that they believe these attacks to be directed at that particular victim and not casual attacks that could have affected anyone. For example P129 mentioned "my colleagues did this [attack] because they are jealous of me" and P142 mentioned "revenge" as a reason for the attack. This phenomenon can be explained in two ways: it could be that the LSA participants are more anxious, suspicious or mistrustful of attackers, or it could be that indeed acts of defamation and revenge are more common within LSA societies.

5.3 Theme 3: Consequences and Reactions to the Attack

The reported consequences of the attacks varied according to the participants' groups. HSA usually reported "no serious consequences". For example, P08 stated "Cas knew private things about Vic, but there were no severe consequences". On a few occasions (5 out of 58), the consequences included reporting

the incident to social network administrators, bank management or even to the police. Around 70% (39 out of 58) of HSA participants also reported that the relationships between the attacker and the victim were affected by the attack. For example, P05 reported that Cas and Vic's relationship after the attack featured "uncomfortableness with Vic keeping more distance".

On the other hand, HSG participants mostly reported "no consequences" (48 out of 61) except in the case of shoulder surfing where they often changed their behavior and became more careful about using their devices in public. For example P70 said that the consequence of these attacks is "Rarely texting in public places" and P85 highlighted "Extra awareness from other possible Cas in the future" as a consequence. They also reported that the relationships were mostly (40 out of 61) unaffected by the attack. For example, when asked about how the relationship was affected P106 replied "not much, since Vic knows that Cas will never stop doing those things, no matter how mad they make Vic".

On the other hand, LSA (39 out of 39) reported the consequences to be more serious and used terms like "loss of trust"(7), "ruined relationships" (12), "defamation" (11) and even "divorce" (1). For example P132 reported that "Vic faced a lot of upsetting encounters from her friends because of the information spread about them". LSA participants (39 out of 39) reported that relationships were strongly affected by attacks with more long term consequences than HSA.

These attacks also influenced the privacy perception of LSA participants more than HSG and HSA participants. HSG participants' majority (40 out of 61) were not influenced by the attacks and their privacy perception did not change. For example, when asked if the situation affected their privacy perception P117 replied saying "No, because I am already cautious". However, around 65% (37 out of 58) of HSA participants had their privacy perception changed after the reported incidents while all LSA participants reported a change of perception. Hacking and physical breach attacks caused the most influence on privacy perception change over other types of attacks.

Finally, when reporting on whether or not the participants viewed the situation as resolved, all attacks involving spouses as the attackers (total of 8 attacks) were perceived as not resolved across the three groups. HSA participants viewed attacks by strangers as mostly resolved, while LSA participants had higher expectations before they can consider an incident to be resolved. For example, they do not consider a situation in which "account access was regained" to be resolved, since this does not undo the implications of the attack. This is likely due to the perceived strong consequences of the attacks. Finally, HSG participants showed no tendency in reporting whether or not attacks were resolved, with almost 50% reporting resolved and 50% unresolved.

5.4 Theme 4: Acceptability of Privacy Invasion

Participants were asked about situations in which they believe privacy invasion is acceptable, e.g., certain individuals whom they would allow to access personal information without considering it a privacy invasion. HSG (22 out of 61) mostly reported that they believe privacy invasion to be justified only in case the safety

of an individual is at stake, or after a person's death. For example P116 mentioned that if "[a] person gone missing, accessing private info might help finding them; law enforcement" it would be acceptable to invade their privacy. On the other hand, HSA were almost equally divided between the acceptance of privacy invasion by parents (11 out of 58) to their children or not accepting privacy invasion at all (13 out of 58). For example, P52 replied "Parent checking on the kids (viewing history of searches and views)". LSA (37 out of 39) mostly did not report any situation where privacy invasion was justified.

Results show that majority of participants (128 out of 156) from the three user groups did not accept personal information access from anyone. Although a few mentioned acceptability from friends, spouses and close family members, the majority believed it to be unjustified. However, around 20% (19 out of 100) of LSA and HSA accepted personal information access from spouses, opposed to 7% among HSG.

5.5 Theme 5: Privacy Invasion Platforms

Participants reported multiple platforms on which privacy invasion incidents took place. Most prominently, privacy invasions occurred on desktop computers (26), laptops (31), tablets (2) and smartphones (71). Most of the privacy invasions in incidents reported by HSG and LSA participants involved smartphones: 51.8% (29 out of 56) of incidents reported by HSGs and 59% (23 out of 39) of those reported by LSAs. On the other hand, HSA participants reported that only 16 incidents out of 53 involved smartphones (30.2%). This difference can be again attributed to the relative less use of public transport by HSA participants, in which the majority of smartphone shoulder surfing takes place [23]. Another possible reason is that LSA users are more likely to have smartphones opposed to other more expensive devices such as tablets, desktops or laptop computers.

6 Discussion

This study investigated privacy invasion experiences and attitudes of 156 participants in Germany, Egypt and Saudi Arabia. Participants in Egypt are divided to those with high socioeconomic status and medium-low socioeconomic status. Findings show differences and similarities among the three groups in all areas of investigation. Table 1 summarizes the results by comparing the differences and similarities experienced across all three participant groups. The first obvious insight is that users from LSA, HSA and HSG have different privacy-related experiences and perceptions, privacy concerns, and privacy requirements.

In this section we discuss the findings in light of prior work, and conclude each subsection with implications for future work in this area.

6.1 LSAs need Usable Privacy Filters

Western cultures are relatively less conservative, and hence implications of photos leaks could be less severe. On the other hand, the Arab culture is governed

by religion and traditions [6, 48]. Revealing personal information is very sensitive and care must be taken to whom it is revealed to. For example, photos especially of women tend to be kept private. Women who send their photos to strangers are frowned upon and their reputation is highly affected. Hence, attackers accessing someone's social network accounts, and taking their photos then claiming that the women have sent them or posting them publicly is very dangerous to a woman's reputation. Also, women who wear headscarfs might exchange photos without their headscarfs with female friends online. If these photos are leaked or retrieved maliciously by an attacker, the victim might be subject to embarrassment, and harassment by friends and family [43, 29].

Implication: Future systems can auto detect private photos using computer vision and machine learning (e.g., detecting the absence of headscarf or intimate moments) and classify them as private ones.

The Arab culture is a collectivist one [29], certain information must be shared with relatives and friends, otherwise the person will be perceived as hiding information, a sign of mistrust in the Arab world. This is the reason why sensitive information might be shared in private messages in the first place.

Implication: This highlights the need for specialized systems that (1) can support these sharing patterns with trusted individuals, while at the same time (2) protect its users from unintended privacy leaks especially those that could have negative implications due to the user's culture, and (3) are usable to accommodate LSA users who could be less tech-savvy than other user groups. These systems need to be accessible for low-literate users. One of the reported problems by LSA users is not knowing how data can be accessed and used against them, or how their privacy can be violated. This prompts for solutions that raise awareness of users. A simple solution that can be applied is providing periodic pop-up notifications for privacy filters that users can apply. This can help users understand the threat associated with this data and how it can be avoided.

6.2 Malicious Privacy Invasions are more Common in LSA Societies

One of the most popular concerns by participants is privacy invasion in online social networks. Participants reported being hacked or leaking sensitive information to attackers. These findings are consistent with previous work which found that 7.1% of Arab respondents to a survey believed that "online social networks might cause troubles" [48]. To combat these effects, Cutillo et al. created Safebook [17]. Safebook is a social network that has an extra layer of safety which stops the creation of fake accounts hence reducing the incidences of impersonation. Safebook also does not allow revealing information about someone by another person unless their consent is received. Another effort to increase safety in social networks is Persona by Baden et al. [10]. Persona emphasizes the role of user in their own privacy by displaying only the information that users explicitly give consent to share.

Black Hat Hacking among LSA LSA experienced more "black hat hacking" than HSA and HSG. This could be due to the fact that the lower socioeconomic

groups hold more to the Arabic traditions than HSA which tends to be more westernized due to exposure to Western education systems and frequent travel [57]. Hence, the reveal of personal information can be very threatening to LSA. Hackers are also more often acquaintances or even family members which shows that these hacks are targeted with the malicious intent of defamation and harm and often motivated by vengeance.

Implication: There should be more emphasis on the insider threat when designing solutions for LSA users [50]. This begs the question of how to balance protection against insider threats while allowing sharing to trusted individuals. This topic requires further research. One potentially interesting direction is having systems communicate to users the potential misuses of their information, or giving users control over the content even when shared beyond the user's first contact (e.g., tell the user if their photo was forwarded, downloaded, or posted somewhere on the web).

Shoulder Surfing is more common in LSA and HSG Results also show that shoulder surfing is experienced more in LSA and HSG. This could be due to the fact that the most common location for shoulder surfing is public transportation [23] and individuals in HSA societies do not use public transportation often, but rather use personal cars and taxis [27].

Implication: Since privacy invasions have serious consequences in LSA, our results confirm the need for privacy protection mechanisms. Many works proposed effective approaches for security and privacy protection yet they are not employed in today's every day technologies. For example, von Zezschwitz et al. [72] proposed mechanisms to protect the visual privacy of photos from shoulder surfing while users browse images on their phones. Eiband et al. [24] proposed protecting text content on mobile devices from shoulder surfing by displaying it in the user's handwriting, which is easy for the legitimate user to understand, but difficult for observers to read. There are many works that protect illegitimate access to social networks [10], and mobile devices (i.e. secure authentication) [71]. Our results confirm that these additional measures for protecting privacy are very important, since they can reduce the potentially severe threats that certain user groups could be subject to.

6.3 Trust is Fragile among Arab Users

LSA viewed the attacks to have more serious consequences, this concurs with the belief that defamation can cause serious damage to this user group [29]. It also shows that preventative measures are very important to accommodate this group. The common preventative technique used offline is trust recommendation. Offline, reputation is held through actions and word of mouth which is maintained in a circle of acquaintances often within a neighbourhood or workplace. This system can be implemented online by building trust recommendation social networks. Other groups show less serious consequences due to the more open minded nature of the relationships and the less malicious nature of the

attacks. The Arab cultures are also more collectivist cultures, that is why they tend to have a more trusting attitude [29]. However, the privacy attacks they experience and the damage caused by these attacks can cause them to lose trust. This loss of trust is conveyed by the change in privacy perception observed in HSA and LSA after the attacks compared to HSG. Attacks from spouses are never perceived as resolved. While attacks from strangers are viewed as resolved in HSA and HSG because once the accounts are regained or the information is dealt with, participants do not expect anything further due to the mild nature of the consequences. On the other hand, LSA do not perceive issues to be resolved since the consequences are very strong.

6.4 Exaggerated Fears

Participants from lower socioeconomic status in Arab countries are usually paranoid about their own safety [47]. They believe that they are constantly being monitored or attacked. This can be due to their limited resources and their fear of not being secure enough, or due to the limited understanding of the security features of technological devices. Therefore, they can easily believe that any attack is directed to them even if it were a mere coincidence. LSA users often think that others are participating in acts of defamation or revenge against them, as suggested by P129 (LSA), who thought others are after her privacy due to jealousy.

While lots of efforts are now directed towards customization for marginalized groups. Some of the techniques and methodologies used may have hidden consequences. For example, participatory design methods are used to tailor designs such as the work done by Weber et al. [64]. However, care must be taken as personalization can make users, and particularly LSA ones, worry or lose trust of the system if it is perceived to be requesting more data than it needs [14]. This can also be counteracted by providing culture-appropriate awareness raising techniques such as privacy filters mentioned above.

6.5 Privacy Invasion Acceptance

In terms of privacy invasion acceptance, participants from LSA did not accept privacy invasion at all. This could be due to the strong consequences that the previous privacy invasion encounters caused. On the other hand, many HSA participants believed that parents can invade children privacy. This is deeply routed in the Arab culture, where parents are perceived as having control and being responsible over all nature of child safety and well-being. This is not reflected in the HSG participants who see only personal safety, national threats and death as acceptable reasons for privacy invasion. The implication of this phenomenon on device access and access modes should be studied.

7 Conclusion and Future Work

In this study, we investigated the privacy invasion perceptions of 156 participants. A survey was conducted online and offline with participants from Germany, Egypt and Saudi Arabia. Egyptian participants were divided between high and medium-low socioeconomic groups. Participants were asked to report privacy invasion incidents they experienced, their feelings and attitudes towards them and how it changed their privacy perception. They were also asked about their acceptability of privacy invasions in special circumstances or by special people. Finally, they were asked about who they protect their privacy from. Participants from LSA experienced more harmful attacks that resulted in stronger consequences on their relationships and reputations. Participants from HSG were more forgiving and experienced milder consequences. However, they showed a change of attitude when it came to attacks of shoulder surfing. Participants from HSA were in the middle of both extremes. They showed some concern about the attacks they faced. In addition, HSA participants believed privacy invasion to be accepted by parents to monitor children, while HSG sometimes believed it to be acceptable in case of safety or death and LSA never believed it to be acceptable. Designs must therefore be customized to each user group to assist them in respecting their privacy and protecting their data.

These results underline that privacy-related experiences, perceptions, concerns and requirements are different between LSA, HSA and HSG societies. This implies that privacy protection mechanisms should be designed with differences between different socioeconomic groups in mind, rather than following a one-size-fits all approach with WEIRD societies in the forefront. Furthermore, we confirm that privacy invasions are more common in LSA societies, and that trust among Arab users is fragile. This emphasizes the importance of trust and privacy protection when designing systems.

Our results highlight the need for usable privacy protection systems that are tailored for each user group. For future work, we plan to study privacy in more Arab cultures, and also investigate similar and different perceptions among the studied groups and users from low socioeconomic groups in WEIRD countries.

References

1. Abokhodair, N., Vieweg, S.: Privacy & social media in the context of the arab gulf. In: Proc. DIS'16. pp. 672–683. ACM (2016)
2. Ahmed, S.I., Guha, S., Rifat, M.R., Shezan, F.H., Dell, N.: Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In: Proc. ICTD '16. pp. 11:1–11:10. ACM (2016), http://doi.acm.org/10.1145/2909609.2909661
3. Ahmed, S.I., Haque, M.R., Chen, J., Dell, N.: Digital privacy challenges with shared mobile phone use in bangladesh. Proc. ACM Hum.-Comput. Interact. **1**(CSCW), 17:1–17:20 (Dec 2017), http://doi.acm.org/10.1145/3134652
4. Ahmed, S.I., Haque, M.R., Guha, S., Rifat, M.R., Dell, N.: Privacy, security, and surveillance in the global south: A study of biometric mobile sim registration in

bangladesh. In: Proc. CHI '17. pp. 906–918. ACM (2017), http://doi.acm.org/10.1145/3025453.3025961
5. Al-Dawood, A., Abokhodair, N., El mimouni, H., Yarosh, S.: "against marrying a stranger": Marital matchmaking technologies in saudi arabia. In: Proc. DIS '17. pp. 1013–1024. ACM (2017), http://doi.acm.org/10.1145/3064663.3064683
6. Alabdulqader, E., Lazem, S., Khamis, M., Dray, S.: Exploring participatory design methods to engage with arab communities. (2018), https://doi.org/10.1145/3170427.3170623
7. Almaney, A.J., Alwan, A.: Communicating with the Arabs: A handbook for the business executive. Waveland Press (1982)
8. Alsheikh, T., Rode, J.A., Lindley, S.E.: (whose) value-sensitive design: A study of long- distance relationships in an arabic cultural context. In: Proc. CSCW '11. pp. 75–84. ACM (2011), http://doi.acm.org/10.1145/1958824.1958836
9. Anderson, L., Wilson, S.: Critical incident technique. (1997)
10. Baden, R., Bender, A., Spring, N., Bhattacharjee, B., Starin, D.: Persona: an online social network with user-defined privacy. In: ACM SIGCOMM Computer Communication Review. vol. 39, pp. 135–146. ACM (2009)
11. Bagnall, J., Bounie, D., Huynh, K.P., Kosse, A., Schmidt, T., Schuh, S.D., Stix, H.: Consumer cash usage: A cross-country comparison with payment diary survey data (2014), https://ssrn.com/abstract=2796990
12. Belk, R., Sobh, R.: Gender and privacy in arab gulf states: Implications for consumption and marketing. Handbook of Islamic marketing pp. 71–96 (2011)
13. Bellman, S., Johnson, E.J., Kobrin, S.J., Lohse, G.L.: International differences in information privacy concerns: A global survey of consumers. The Information Society **20**(5), 313–324 (2004)
14. Briggs, P., Simpson, B., De Angeli, A.: Personalisation and trust: a reciprocal relationship? In: Designing Personalized user experiences in eCommerce, pp. 39–55. Springer (2004)
15. Ching, C.C., Basham, J.D., Jang, E.: The legacy of the digital divide: Gender, socioeconomic status, and early exposure as predictors of full-spectrum technology use among young adults. Urban Education **40**(4), 394–411 (2005)
16. Clemmensen, T., Roese, K.: An overview of a decade of journal publications about culture and human-computer interaction (hci). In: Katre, D., Orngreen, R., Yammiyavar, P., Clemmensen, T. (eds.) Human Work Interaction Design: Usability in Social, Cultural and Organizational Contexts. pp. 98–112. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
17. Cutillo, L.A., Molva, R., Strufe, T.: Safebook: A privacy-preserving online social network leveraging on real-life trust. IEEE Communications Magazine **47**(12) (2009)
18. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I.: Internet users privacy concerns and beliefs about government surveillance. Journal of Global Information Management **14**(4), 57–93 (2006). https://doi.org/10.4018/jgim.2006100103
19. Dunning, D., Heath, C., Suls, J.M.: Flawed self-assessment: Implications for health, education, and the workplace. Psychological science in the public interest **5**(3), 69–106 (2004)
20. Edwards, A.L.: The social desirability variable in personality assessment and research. (1957)
21. Egelman, S., Jain, S., Portnoff, R.S., Liao, K., Consolvo, S., Wagner, D.: Are you ready to lock? In: Proc. CCS'14. pp. 750–761. ACM (2014), http://doi.acm.org/10.1145/2660267.2660273

22. Egelman, S., Peer, E.: The myth of the average user: Improving privacy and security systems through individualization. In: Proc. NSPW '15. pp. 16–28. ACM (2015), http://doi.acm.org/10.1145/2841113.2841115
23. Eiband, M., Khamis, M., von Zezschwitz, E., Hussmann, H., Alt, F.: Understanding shoulder surfing in the wild: Stories from users and observers. In: Proc. CHI '17. pp. 4254–4265. ACM (2017), http://doi.acm.org/10.1145/3025453.3025636
24. Eiband, M., von Zezschwitz, E., Buschek, D., Hussmann, H.: My scrawl hides it all: Protecting text messages against shoulder surfing with handwritten fonts. In: Proc. CHI EA '16. pp. 2041–2048. ACM (2016), http://doi.acm.org/10.1145/2851581.2892511
25. El-Gilany, A., El-Wehady, A., El-Wasify, M.: Updating and validation of the socioeconomic status scale for health research in egypt/mise à jour et validation d'une échelle du statut socioéconomique pour la recherche en santé en égypte. Eastern Mediterranean Health Journal **18**(9), 962 (2012)
26. El-Gilany, A.H., Amr, M., Hammad, S.: Perceived stress among male medical students in Egypt and Saudi Arabia: effect of sociodemographic factors. Ann Saudi Med **28**(6), 442–448 (2008)
27. Elias, W., Shiftan, Y.: The influence of individual's risk perception and attitudes on travel behavior. Transportation Research Part A: Policy and Practice **46**(8), 1241 – 1251 (2012), http://www.sciencedirect.com/science/article/pii/S0965856412000882
28. Fahmy, S.: Determining simple parameters for social classifications for health research. Bull High Inst Public Health **13**, 95–108 (1983)
29. Feghali, E.: Arab cultural communication patterns. International Journal of Intercultural Relations **21**(3), 345–378 (1997)
30. Finardi, U., Buratti, A.: Scientific collaboration framework of brics countries: an analysis of international coauthorship. Scientometrics **109**(1), 433–446 (Oct 2016). https://doi.org/10.1007/s11192-016-1927-0, https://doi.org/10.1007/s11192-016-1927-0
31. Group, M.M.: Internet world stats. https://www.internetworldstats.com/stats.htm, accessed 18 September 2018
32. Guest, G., MacQueen, K.M., Namey, E.E.: Applied thematic analysis. Sage Publications (2011)
33. Harbach, M., De Luca, A., Malkin, N., Egelman, S.: Keep on lockin' in the free world: A multi-national comparison of smartphone locking. In: Proc. CHI '16. pp. 4823–4827. ACM (2016), http://doi.acm.org/10.1145/2858036.2858273
34. Harbach, M., Fahl, S., Smith, M.: Who's afraid of which bad wolf? a survey of it security risk awareness. In: Proc. IEEE CSF'14. pp. 97–110 (July 2014). https://doi.org/10.1109/CSF.2014.15
35. Harbach, M., von Zezschwitz, E., Fichtner, A., Luca, A.D., Smith, M.: It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In: Proc. SOUPS '14. pp. 213–230. USENIX Association (2014), https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach
36. Henrich, J., Heine, S.J., Norenzayan, A.: Most people are not weird. Nature **466**(7302), 29–29 (Jul 1 2010)
37. Henrich, J., Heine, S.J., Norenzayan, A.: The weirdest people in the world? Behavioral and Brain Sciences **33**(2-3), 61–83 (2010), https://www.ncbi.nlm.nih.gov/pubmed/20550733
38. Jones, M., Robinson, S., Pearson, J., Joshi, M., Raju, D., Mbogo, C.C., Wangari, S., Joshi, A., Cutrell, E., Harper, R.: Beyond "yesterday's tomorrow": Future-focused

mobile interaction design by and for emergent users. Personal Ubiquitous Comput. **21**(1), 157–171 (Feb 2017), https://doi.org/10.1007/s00779-016-0982-0
39. Karlson, A.K., Brush, A., Schechter, S.: Can i borrow your phone?: understanding concerns when sharing mobile phones. In: Proc. CHI'09. pp. 1647–1650. ACM (2009)
40. Kelley, E.E., Motika, F., Motika, P.V., Motika, E.M.: Secure credit card (Nov 4 2003), uS Patent 6,641,050
41. Lazem, S., Jad, H.A.: We play we learn: Exploring the value of digital educational games in rural egypt. In: Proc. CHI '17. pp. 2782–2791. ACM (2017), http://doi.acm.org/10.1145/3025453.3025593
42. Lee, I., Choi, B., Kim, J., Hong, S.J.: Culture-technology fit: Effects of cultural characteristics on the post-adoption beliefs of mobile internet users. International Journal of Electronic Commerce **11**(4), 11–51 (2007)
43. Levmore, S., Nussbaum, M.C.: The offensive internet. Harvard University Press (2010)
44. Li, Y., Kobsa, A., Knijnenburg, B.P., Nguyen, M.C.: Cross-cultural privacy prediction. Proceedings on Privacy Enhancing Technologies **2017**(2), 113–132 (2017)
45. Marques, D., Guerreiro, T., Carriço, L.: Measuring snooping behavior with surveys: it's how you ask it. In: Proc. CHI EA '14. pp. 2479–2484. ACM (2014)
46. Miles, M.B., Huberman, A.M., Huberman, M.A., Huberman, M.: Qualitative data analysis: An expanded sourcebook. sage (1994)
47. Mirowsky, J., Ross, C.E.: Paranoia and the structure of powerlessness. American Sociological Review pp. 228–239 (1983)
48. Mohamed, A.A.A.: Online privacy concerns among social networks' users/question concernant les affaires personnelles des utilisateurs de réseaux sociaux en ligne. Cross-cultural communication **6**(4), 74 (2010)
49. Mounir, H.: Only 33% of egyptian adults own bank accounts: deputy cbe governor. https://dailynewsegypt.com/2017/10/24/33-egyptian-adults-bank-accounts-deputy-cbe-governor/ (2017), accessed 18 September 2018
50. Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., Beznosov, K.: Know your enemy: The risk of unauthorized access in smartphones by insiders. In: Proc. MobileHCI '13. pp. 271–280. ACM (2013), http://doi.acm.org/10.1145/2493190.2493223
51. Nassir, S., Leong, T.W.: Traversing boundaries: Understanding the experiences of ageing saudis. In: Proc. CHI '17. pp. 6386–6397. ACM (2017), http://doi.acm.org/10.1145/3025453.3025618
52. Nobles, A.Y., Sciarra, D.T.: Cultural determinants in the treatment of arab americans: A primer for mainstream therapists. American Journal of Orthopsychiatry **70**(2), 182 (2000)
53. Robinson, S., Pearson, J., Reitmaier, T., Ahire, S., Jones, M.: Make yourself at phone: Reimagining mobile interaction architectures with emergent users. In: Proc. CHI '18. pp. 407:1–407:12. ACM (2018), http://doi.acm.org/10.1145/3173574.3173981
54. Saleh, M., Khamis, M., Sturm, C.: Privacy invasion experiences and perceptions: A comparison between germany and the arab world. In: Proc. CHI EA '18. ACM (2018), http://doi.acm.org/10.1145/3170427.3188671
55. Sambasivan, N., Checkley, G., Batool, A., Ahmed, N., Nemer, D., Gaytán-Lugo, L.S., Matthews, T., Consolvo, S., Churchill, E.: "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In: Proc. SOUPS '18. pp. 127–142. USENIX Association (2018), https://www.usenix.org/conference/soups2018/presentation/sambasivan

56. Sambasivan, N., Jain, N., Checkley, G., Baki, A., Herr, T.: A framework for technology design for emerging markets. Interactions **24**(3), 70–73 (Apr 2017), http://doi.acm.org/10.1145/3058496
57. Sayed, F.H.: Transforming education in Egypt: Western influence and domestic policy reform. American Univ in Cairo Press (2006)
58. Schwartz, B.: The social psychology of privacy. American Journal of Sociology **73**(6), 741–752 (1968)
59. Solove, D.J.: Speech, privacy, and reputation on the internet. Lovmore S., Nussbaum M.(2010), The offensive Internet (2010)
60. Sturm, C., Oh, A., Linxen, S., Abdelnour Nocera, J., Dray, S., Reinecke, K.: How weird is hci?: Extending hci principles to other countries and cultures. In: Proc. CHI EA '15. pp. 2425–2428. ACM (2015), http://doi.acm.org/10.1145/2702613.2702656
61. Sunstein, C.: Believing false rumors. The (2010)
62. Talhouk, R., Mesmar, S., Thieme, A., Balaam, M., Olivier, P., Akik, C., Ghattas, H.: Syrian refugees and digital health in lebanon: Opportunities for improving antenatal health. In: Proc. CHI '16. pp. 331–342. ACM (2016), http://doi.acm.org/10.1145/2858036.2858331
63. Wang, P., Petrison, L.A.: Direct marketing activities and personal privacy: A consumer survey. Journal of Direct Marketing **7**(1), 7–19 (1993)
64. Weber, S., Harbach, M., Smith, M.: Participatory design for security-related user interfaces. Proc. USEC **15** (2015)
65. Westin, A.F., Ruebhausen, O.M.: Privacy and freedom. Ig Publishing (2015)
66. Wilkinson, D., Namara, M., Badillo-Urquiola, K., Wisniewski, P., Knijnenburg, B., Page, X., Toch, E., Romano-Bergstrom, J.: Moving beyond a "one-size fits all" approach: Exploring individual differences in privacy (2018), https://doi.org/10.1145/3170427.3170617
67. Wisniewski, P., Islam, A.N., Knijnenburg, B.P., Patil, S.: Give social network users the privacy they want. In: Proc. CSCW '15. pp. 1427–1441. ACM (2015), http://doi.acm.org/10.1145/2675133.2675256
68. Wisniewski, P.J., Knijnenburg, B.P., Lipford, H.R.: Making privacy personal: Profiling social network users to inform privacy education and nudging. International Journal of Human-Computer Studies **98**, 95 – 108 (2017), http://www.sciencedirect.com/science/article/pii/S1071581916301185
69. Yardi, S., Bruckman, A.: Income, race, and class: Exploring socioeconomic differences in family technology use. In: Proc. CHI '12. pp. 3041–3050. ACM (2012), http://doi.acm.org/10.1145/2207676.2208716
70. Yoo, C.W., Ahn, H.J., Rao, H.R.: An exploration of the impact of information privacy invasion (2012)
71. von Zezschwitz, E., De Luca, A., Brunkow, B., Hussmann, H.: Swipin: Fast and secure pin-entry on smartphones. In: Proc. CHI '15. pp. 1403–1406. ACM (2015), http://doi.acm.org/10.1145/2702123.2702212
72. von Zezschwitz, E., Ebbinghaus, S., Hussmann, H., De Luca, A.: You can't watch this!: Privacy-respectful photo browsing on smartphones. In: Proc. CHI '16. pp. 4320–4324. ACM (2016), http://doi.acm.org/10.1145/2858036.2858120