Privacy Invasion Experiences and Perceptions: A comparison between Germany and the Arab World

Mennatallah Saleh
[1]Hamm-Lippstadt University of Applied Science, Germany
[2]Technical University of Berlin, Germany
Menna.eSaleh@gmail.com

Mohamed Khamis
LMU Munich, Germany
Mohamed.Khamis@ifi.lmu.de

Christian Sturm
Hamm-Lippstadt University of Applied Science, Germany
Christian.Sturm@hshl.de

CHI'18 Extended Abstracts, April 21–26, 2018, Montreal, QC, Canada
ACM 978-1-4503-5621-3/18/04.
https://doi.org/10.1145/3170427.3188671

Abstract
Similar to research in behavioral psychology, research in privacy and usable security has focused mainly on Western, Educated, Industrialized, Rich, and Democratic (WEIRD) societies. This excludes a large portion of the population affected by privacy implications of technology. In this work, we report on a survey (N=117) in which we studied technology-related privacy concerns of users from different countries, including developing countries such as Egypt, and Saudi Arabia, and developed countries such as Germany. By comparing results from those countries, and relating our findings to previous work, we brought forth multiple novel insights that are specific to privacy of users from under-investigated countries. We discuss the implications of our findings on the design of privacy protection mechanisms.

Author Keywords
Privacy invasion; security; shoulder surfing; Arab world

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous; K.6.4 [Security and Protection]

Introduction
Researchers from psychology, economics and cognitive science came to a conclusion that much of the research done in these areas considered subjects who are mainly from

Western, Industrialized, Rich, and Democratic (WEIRD) populations [13]. Henrich et al. [13] brought the community's attention to that fact, and argued that a WEIRD society is often a psychological outlier.

Research in privacy and usable security is not an exception; most of the existing work explored privacy concerns in developed countries only. This means that there might be novel privacy concerns that have not been studied in depth yet. For example, privacy invasions in countries with political turbulence might have lethal consequences, or certain individuals might believe they have the right to invade a certain family member's privacy in some societies.

To expand our knowledge of privacy concerns, we explore the privacy needs of technology users from different countries through a survey (N=117) that was distributed mainly in Egypt, Saudi Arabia, and Germany. By comparing the the results from Arab and German societies, and by contrasting the findings to previous work, we extracted a set of novel insights. For example, we found out that shoulder surfing is less common in Arab societies compared to Germany, but credit card theft and hacking are more common in the former. Our long term aim is to investigate the needs of under represented user groups.

Related Work

We are not the first to investigate privacy requirements across multiple countries. Multiple works explored privacy needs, perceptions, and security-related behavior. Most notably, Harbach et al. collected survey responses from 8286 participants from 8 different countries, including Australia, Canada, Germany, Italy, Japan, Netherlands, the UK, and the US [10]. They found that compared to participants from other countries, Japanese participants considered data on their smartphones to be more sensitive, and German ones were more likely to find protecting access to their phones to be important. Dinev et al. compared the perceptions of privacy about government surveillance across Internet users from USA and Italy [3]. They found that participants from Italy had lower privacy concerns, and lower perceived need for government surveillance compared to those form USA. In another study, Harbach et al. compared risk perceptions across USA and Germany [11]. They found that participants from USA had greater fear of identity theft, while German participants were more concerned about hidden costs in services, as well as frauds and scams in online shopping. More recently, Eiband et al. collected real shoulder surfing stories from participants from different countries [6]. The main bulk of participants came from Germany and Egypt, but they also had few participants from the USA, Bulgaria, India, Italy, Romania, Russia and South Korea. Their main aim was to find real 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.

The cross-cultural and multi-national comparisons reported in the aforementioned works highlight the vast differences in privacy perception across different countries. However, all of the comparisons involved WEIRD countries with the exception of Eiband et al.'s survey about shoulder surfing [6]. But even Eiband et al. did not investigate differences across participants from different countries, and they focused solely on shoulder surfing while we look into privacy in technology use in general. Thus, the novelty of our work lies in the explicit focus on technology-related privacy perceptions of users from Arab societies.

Questionnaire Development

A questionnaire was created to collect experiences with privacy violations, privacy perceptions and privacy influences. It was distributed online through social media and

university mailing lists. The questionnaire was distributed to German participants and Arab participants (Egyptian and Saudis) residing in their own countries to ensure that no external cultural influences affected the results.These countries were selected because they had the most number of internet users in their region: Germany (72 million), Egypt (37 million) and Saudi Arabia (24 million) [8].

Questionnaire Design and Limitations

The aim of the questionnaire was to collect data about privacy invasion incidents and perceptions. Results annonymity was emphasized for topic sensitivity. We relied on recall of a particular incident to investigate what participants felt and believed about privacy invasion. No negative connotations were used throughout the questionnaire and the terms victim and attacker were replaced by gender neutral personas “Vic” and “Cas” respectively. Gender neutral pronouns have been used in studies to avoid participant misunderstanding, most recently by Eiband et al. [6] Two iterations of pre-study were conducted where the questionnaire was given to 6 participants and their feedback about understanding the questionnaire and questionnaire organization was taken into consideration. As with all questionnaires, one of the limitations is the bias of self-report [5]. In addition, due to the sensitivity of the topic, social desirability may have been displayed. Despite our attempt to make the description neutral, participants may have not been comfortable describing themselves as the attacker (“Cas“) or would have preferred reporting situations where they were victims or observers; only 15% of participants reported themselves as attackers.

Questionnaire Structure

The questionnaire was divided into five sections. The first section collected a particular privacy invasion experience of the participant to be the focus of the questionnaire onwards. Participants were asked to freely recollect a privacy invasion incident and their feelings about this incident. In case participants didn’t have any incidents to recall, their answers were discarded for Section 1 and 2. In the next sections, more details were collected about the incident, such as the victim’s feeling, type of information accessed, location of incidence and how it influenced the privacy perception of the participant. We asked participants about their perceived justifications for privacy invasions: whether they believed it is acceptable for special situations or individuals to access their private data. Finally, the last section collected participant demographics. Participants were asked to rate the honesty of their replies through a five-point Likert scale to help exclude invalid data [16].

Results and Discussion

Overall we collected a total of 117 responses. 31 participants were males, 79 were females, and 7 did not report their gender. We collected 56 responses by participants from western countries. The biggest group was from Germany (49 participants). While 54 responses were by participants from Arab countries, including Egypt (30 participants), and Saudi Arabia (22 participants). Participants ages were between 18-57 with a mean age of 30 (SD=10.6). Participants were compensated with shopping vouchers or credit points for their studies.

Types of Experienced Privacy Invasions

We classified the reported stories to 12 categories based on attacks defined in previous work related to social networks [2], shoulder surfing [6], and mobile device sharing/borrowing [14]. We further added credit card theft and involuntary privacy invasions. In some cases, the story would fit into several categories. For example, P80 reported that because a friend used the same password on several platform, his online account was stolen and the attacker

was able to gain access to the victim's Facebook, Amazon, and Google Mail accounts. From there the attacker started defaming the victim and spreading phishing emails. In that case, this story was classified as an instance of each of: identify theft, defamation, and hacking. Figure 1 illustrates the distribution of the reported stories across participants from Germany and Arab countries.

Notable differences can be seen in cases of shoulder surfing, with participants Germany experiencing slightly more shoulder surfing situations. Eiband et al. [6] reported that shoulder surfing occurs most often in public transport. Our questionnaire distribution approach, as well as collected data about the education, residence area, and income of our participants indicate that our sample belongs mainly to medium-to-high socio-economic subgroups in each country; in Germany, all classes of society use public transport, while in Egypt and Saudi Arabia, public transport is not common for individuals that belong to medium to high socio-economic subgroups [7]. Hence, a possible reason for lower shoulder surfing cases in Egypt and Saudi Arabia is that our sample group do not often use public transport.

Participants from Egypt and Saudi Arabia have more negative experiences with credit card theft. This might be attributed to two reasons. First, a possibility is the weak credit card regulations in Egypt and Saudi Arabia, in which it is the user's responsibility to bear the expenses in case of a fraud. As a result, credit card users from Egypt and Saudi Arabia are likely to face more negative experiences, and this might have resulted in an increased recall bias towards these events. Second, it is known that credit card usage is not as popular in Germany as in other countries such as the United States [11], and that Germans tend to prefer cash transactions [1]. While we could not find direct comparisons between credit card usage in the countries involved in our

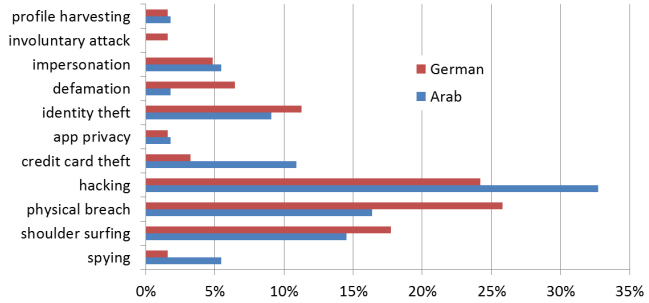

Figure 1: A categorization of reported privacy invasions revealed some tendencies.

research, we assume that a reason for experiencing less credit card thefts is that our German participants do not use them as often.

Privacy Invasion Platforms

Previous work that investigated shoulder surfing focused mostly on smartphones and handheld devices [6, 9, 10, 12]. We found that other forms of mobile devices, such as laptops, are also vulnerable to privacy invasions albeit less common compared to handheld mobile devices. We collected 48 privacy invasion stories involving smartphones, 28 involving laptop computers, and 16 involving desktop computers. The rest were distributed among tablets, ATMs. More than half of the responses by German participants (55.8%) involved handheld mobile devices, such as smartphones. This percentage dropped to 36.4% when considering stories by Arab participants only. In contrast, more stories by Arabs involved laptops (34.1%). While laptops were subject to privacy invasion only in 21.2% of the stories reported by Germans. The bias towards smartphones in stories by participants from Germany can be explained by the same reasons we clarified earlier, related to the use of public transport. These results suggest that privacy protec-

tion measures should not only consider mobile devices, but also laptops and stationary devices such as desktops.

Reactions to Privacy Invasions are more Severe in Arab Countries

When asked if their perception of privacy was influenced by the incident, participants from Arab countries showed a tendency to be influenced more often (83.8%) compared to those from Germany (67.4%). For example, P10 was a 27 years old female from Egypt. She reported an incident where someone created a fake Facebook profile using her name and pictures, and then started sending defaming messages to the victim's friends. P10 mentioned that she became more privacy aware; she revised the privacy settings of her account, added profile restrictions, removed acquaintances from the friends list, deleted all important and sensitive messages, and activated 2-step authentication. We expect that the reason behind the more severe reactions by participants from Arab countries, is that these societies are often describe as collectivist cultures, in which fame and reputation are highly valued [4].

When is Privacy Invasion Justified?

When asked if they would consider privacy violation to be justified in certain situations, the majority of participants from Germany highlighted situations where safety is a concern. For example, P59 was a 20 year old from Germany. He stated "For example, if there is reasonable suspicion that the person in question is in danger I think that their safety always comes prior to their privacy". On the other hand, participants from Arab countries were more inclined to find a parents' invasion of children's privacy to be justified. For example, we collected 11 opinions (9 females) from participants who come from Arab countries that affirmed this. Participants thought it is justified to monitor "underage children" P29, "son's mobile [phone]" P41, "children or teens to protect them" P47. These views were common across participants from: Saudi Arabia; P46 finds it justified to invade privacy of children "If the parent, sibling suspect that their kid, sibling is in danger or being harassed", as well as those from Egypt; P48 thinks it is justified "if someone is worried about the wellbeing or behaviour of their loved ones. I wouldn't do it with a spouse but I would with kids if I were worried they were endangering themselves.".

Children's privacy is a controversial topic. It is important to design privacy protection knowing that. In one view, preventing harm to the child is the priority, but the harm of infringing on a child's privacy should also be taken into account [15]. Privacy protection mechanisms should be designed with this in mind; how exactly such mechanisms can be implemented requires an in-depth investigation.

Conclusion and Future Work

In this work, we reported on our preliminary analysis of 117 survey responses in which we studied technology-related privacy invasions of users from different countries. We focused on comparing privacy situations and perceptions in Egypt, Saudi Arabia and Germany. We noticed some differences due to the collectivist nature of Arab communities, their sensitivity to reputation, and the lower popularity of public transport This work only focuses on three countries, it needs to be extended to be more representative of the diversity the Arab world carries.. We also plan to extend it by in-depth interviews on privacy perceptions and how privacy violations affect them.

REFERENCES

1. John Bagnall, David Bounie, Kim P. Huynh, Anneke Kosse, Tobias Schmidt, Scott D. Schuh, and Helmut Stix. 2014. Consumer Cash Usage: A Cross-Country Comparison with Payment Diary Survey Data. (2014).

2. Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. 2009. Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Magazine* 47, 12 (2009).

3. Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, and Ilaria Serra. 2006. Internet Users Privacy Concerns and Beliefs About Government Surveillance. *Journal of Global Information Management* 14, 4 (2006), 57–93.

4. Peter C. Dodd. 1973. Family Honor and the Forces of Change in Arab Society. *International Journal of Middle East Studies* 4, 1 (1973), 40–54.

5. David Dunning, Chip Heath, and Jerry M Suls. 2004. Flawed self-assessment: Implications for health, education, and the workplace. *Psychological science in the public interest* 5, 3 (2004), 69–106.

6. Malin Eiband, Mohamed Khamis, Emanuel von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding Shoulder Surfing in the Wild: Stories from Users and Observers. In *Proc. CHI'17*. ACM, New York, NY, USA, 4254–4265.

7. Wafa Elias and Yoram Shiftan. 2012. The influence of individual's risk perception and attitudes on travel behavior. *Transportation Research Part A: Policy and Practice* 46, 8 (2012), 1241 – 1251. http://www.sciencedirect.com/science/article/pii/S0965856412000882

8. Miniwatts Marketing Group. 2018. Internet World Stats. https://www.internetworldstats.com/stats.htm. (2018). Accessed: 2018-02-15.

9. Marian Harbach, Alexander De Luca, and Serge Egelman. 2016a. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proc. CHI'16*. ACM, New York, NY, USA, 4806–4817.

10. Marian Harbach, Alexander De Luca, Nathan Malkin, and Serge Egelman. 2016b. Keep on Lockin' in the Free World: A Multi-National Comparison of Smartphone Locking. In *Proc. CHI'16*. ACM, New York, NY, USA, 4823–4827.

11. Marian Harbach, Sascha Fahl, and Matthew Smith. 2014a. Who's Afraid of Which Bad Wolf? A Survey of IT Security Risk Awareness. In *Proc. IEEE CSF'14*. 97–110.

12. Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014b. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Proc. SOUPS'14*. USENIX Association, Menlo Park, CA, 213–230.

13. Joseph Henrich, Steven J Heine, and Ara Norenzayan. 2010. The weirdest people in the world? *Behavioral and Brain Sciences* 33, 2-3 (2010), 61–83.

14. Amy K Karlson, AJ Brush, and Stuart Schechter. 2009. Can i borrow your phone?: understanding concerns when sharing mobile phones. In *Proc. CHI'09*. ACM, 1647–1650.

15. Benjamin Shmueli and Ayelet Blecher-Prigat. 2010. Privacy for children. *Colum. Hum. Rts. L. Rev.* 42 (2010), 759–796.

16. Emanuel Von Zezschwitz, Alexander De Luca, Philipp Janssen, and Heinrich Hussmann. 2015. Easy to draw, but hard to trace?: On the observability of grid-based (un) lock patterns. In *Proc. CHI'15*. ACM, 2339–2342.