Keep on Lockin' in the Free World:

A Multi-National Comparison of Smartphone Locking

Marian Harbach[1], **Alexander De Luca**[2], **Nathan Malkin**[3], **Serge Egelman**[1,3]
[1]International Computer Science Institute, Berkeley, CA
[2]Google, Zurich, Switzerland
[3]University of California, Berkeley, CA
mharbach@icsi.berkeley.edu, adeluca@google.com, {nmalkin,egelman}@cs.berkeley.edu

ABSTRACT
We present the results of an online survey of smartphone unlocking ($N = 8,286$) that we conducted in eight different countries. The goal was to investigate differences in attitudes towards smartphone unlocking between different national cultures. Our results show that there are indeed significant differences across a range of categories. For instance, participants in Japan considered the data on their smartphones to be much more sensitive than those in other countries, and respondents in Germany were 4.5 times more likely than others to say that protecting data on their smartphones was important. The results of this study shed light on how motivations to use various security mechanisms are likely to differ from country to country.

Author Keywords
Smartphone security; lock screen; multi-national survey

ACM Classification Keywords
D.4.6. Operating Systems: Security and Protection—*Authentication*; H.5.2. Information Interfaces and Presentation: User Interfaces—*User-centered design*

INTRODUCTION
Recent studies of real-world smartphone unlocking behavior have shed light on whether and why people choose to protect the data on their smartphones [5, 6, 11], such as by using a PIN, pattern, or biometric (e.g., fingerprint). Across all of these studies, participants cited a range of seemingly legitimate—albeit incorrect—justifications for not opting to secure their devices. For instance, in the most common case, the absence of an apparent threat was one of the main factors cited for not protecting a device: many users simply do not consider their data to be sensitive enough to protect. All studies highlight the need for proper protection of devices with secure and usable authentication mechanisms, as well as the need to find ways of motivating users to enable them.

CHI'16, May 07-12, 2016, San Jose, CA, USA
ACM 978-1-4503-3362-7/16/05.
http://dx.doi.org/10.1145/2858036.2858273

However, these studies were conducted on populations in Germany and the U.S. and thus provide only limited generalizability with respect to smartphone unlock behavior on a global scale. From related fields, such as privacy concern research, we know that attitudes do differ between countries and cultures (e.g., [4]), and we assume this is also the case for smartphone locking. Thus, to improve the adoption of better security practices worldwide, we must first gain a better understanding of users' motivations. In order to fill this gap, we conducted a survey with 8,286 participants in 8 countries: Australia, Canada, Germany, Italy, Japan, Netherlands, the United Kingdom, and the United States.

The results show that there are indeed differences between people in different countries. Overall, as in previous studies, convenience as well as absence of perceived threats were among the main reasons for not locking devices. However, specific reasons differed significantly between countries. For instance, German participants, despite ranking the sensitivity of their data lower than Italians and Japanese, were 4.5 times more likely to refer to protection being important in general. While we can only speculate about what causes the differences we observe, our data clearly provides evidence that cultural differences need to be taken into account when trying to nudge users towards adopting security measures.

METHOD
The goal of this study was to investigate inter-country differences in how people use, and think about, smartphone lock screens. In particular, we aimed to answer the following:

1. Does adoption of secure smartphone locking mechanisms differ by country?
2. Do people in different countries differ in their motivations?
3. Are potential differences explained by varying perceptions of the sensitivity of the data on the phone?

To answer these questions, we distributed a survey through Google Consumer Surveys (GCS). The GCS platform is well suited for providing the necessary insights, since it allows us to directly target smartphone users across the eight countries mentioned above. Furthermore, GCS provides a sample of the population that has been shown to be at least as accurate and representative as existing Internet-based panels [9]. A limitation of this service is that it excludes iOS users, and as a result, our study focuses on Android users.

When targeting smartphone users in GCS, surveys will be displayed in the dedicated "Google opinion rewards" app, which allows participants to earn credit for the Google Play store by answering short surveys. In contrast to the inference approach used in the traditional web-based GCS surveys, mobile app users provide basic demographics themselves. This should yield a better sample, since users are stratified based on their demographic information.

Participants in the survey answered three questions:

1. What secret unlock method do you use on your smartphone? [multiple choice]
2. Why did you decide (not) to protect your smartphone with a security mechanism (e.g., a 4-digit PIN)? [open-ended]
3. How sensitive is the information stored on your smartphone? [7-point scale, 7=very sensitive]

The first question was used to divide participants into those who use a secure unlock method (SU group) and those who only use slide-to-unlock or a similar method (StU group). The response to this question determined the next question.

We translated this survey into German, Italian, Dutch, and Japanese. For each language, we consulted two domain experts who were also native speakers in the target language. After both agreed on a translation, we asked acquaintances and Mechanical Turk (MTurk) workers to translate each question and response back to English, without disclosing the original English text. We asked MTurk workers to translate idioms to check for native language proficiency. We solicited at least 5 back-translations for each language and found that they were all semantically identical to the initial English.

After validating the translations, we commissioned 16 GCS surveys. We used two for each country – one for the SU group and one for the StU group – as GCS performs screening instead of branching. We piloted each survey with 30 participants to check for remaining comprehension issues. After finding none, we deployed all 16 surveys simultaneously on July 14, 2015 to collect 500 responses from each condition and country. Data collection concluded within a few days.

Before analyzing the results, open-ended answers for the second question needed to be translated and coded. For translation, we hired two independent professional translators for each language. Following the approach used to translate survey questions and the recommendations of Behr [1], they translated all responses individually and then resolved conflicts in a discussion. The authors themselves and acquaintances proficient in the respective languages conducted random spot-checks to confirm the validity of the translations.

We chose a quantitative content analysis approach and aligned our coding so that we would be able to compare counts of codes between countries. As reasons for choosing a lock screen have been studied in two previous papers [5, 6], we combined the codebooks of these studies as a basis for our coding, which is a common approach [10]. We structured codes to capture individual aspects of responses, such as concerns over specific information, attackers, or scenarios. Most of our codes are in the appendix of Harbach *et al.* [6].

Responses in the SU and StU groups were coded with the respective codebook, allowing for multiple codes for each response. Two experienced coders individually went through every response across all countries and coded them independently. They were instructed to create new codes where necessary to accommodate new themes. Upon completion, coders discussed conflicting codes and resolved all remaining discrepancies. Before conflict resolution, we calculated Kupper-Hafner agreement as a substitute for the traditional Kappa inter-rater agreement [8], given that we used multiple codes per response. Agreement was 0.70 in the SU group and 0.79 for the StU group, indicating substantial agreement.

Statistical Analysis

For simple analyses of contingency tables of demographic properties between countries, we used omnibus chi-square tests before inspecting standardized residuals within the cells. We report absolute values of two or larger as significant effects. To account for demographic covariates (age and gender) when looking at answers to questions one and two, we fitted logistic regression models. For each fitted model, we chose the combination of factors that yielded a significant improvement over the previous model using a chi-square test on the deviance table. Responses to question one were binary coded as secure vs. insecure locking method. For coded responses, presence of a code from the codebook was dummy coded per participant and used as the outcome variable. We then fit models for each of the code categories if an omnibus Pearson's chi-square test was significant on the respective contingency table. We used the United States as reference category for the models and conducted Wald's tests on the group of dummy variables to determine omnibus significance of categorical variables. We then only report those estimates that are significantly different from 0 individually. Lastly, we used ANCOVA to test for differences between the numeric scale-responses of question three, again accounting for differences in age and gender between countries.

RESULTS

Overall, we collected screening responses from 21,451 participants. As GCS oversamples each of its strata to allow for timely completion, we received 8,286 complete responses to our three-question survey. For the main analysis, we use the first 500 responses from each condition in each of the eight countries, for a total of 8,000 responses.

Having a Secure Lock Screen

To answer our first research question, we looked at all 21,451 participants that completed the screener question. Almost half (48.5 %) of these were female (with 0.2 % unknown) and 55 % were younger than 35 years (24.2 % between 18 and 24, 25.1 % between 35 and 44, .08 % unknown). However, these values were significantly different between countries (Age: $\chi^2_{42} = 1209$, $p < .0001$, Gender: $\chi^2_{14} = 247$, $p < .0001$). For example, participants from Japan fell into older age categories much more frequently, while Australian and Canadian participants were younger. The Australian and Japanese sample also held more males while the Italian and Dutch sample skewed towards more female respondents.

Variable	Estimate	Std. Err.	z	Odds Ratio
Intercept	.606	.054	11.18*	
country=AU	.326	.062	5.26*	1.39
country=CA	.270	.062	4.35*	1.31
country=DE	.409	.060	6.74*	1.51
country=IT	-.556	.057	-9.73*	0.57
country=JP	.067	.061	1.09	
country=NL	.306	.059	5.18*	1.36
country=UK	.565	.062	9.16*	1.76
group=SU	-.039	.032	-1.21	
Age=25-34	-.175	.042	-4.20*	.84
Age=35-44	-.159	.044	-3.66*	.85
Age=45-54	-.204	.051	-3.98*	.82
Age=55-64	-.407	.072	-5.66*	.66
Age=65+	-.530	.127	-4.17*	.59
Age=Unknown	-1.112	.659	-1.688	
Gender=Male	.323	.030	10.71*	1.38
Gender=Unknown	1.022	.461	2.21*	2.78

Table 1. Logistic regression model: likelihood of using a secure lock screen by country, age, and gender. An * denotes significance ($p < .05$).

We fit a logistic regression model to predict whether or not users will have a secure lock screen based on country. To check for irregularities, we also included the group this user was screened for (SU vs. StU) in the model. Finally we included age and gender to account for the above differences. All main effects were significant, except for the user group. Table 1 gives an overview of the fitted model and Table 4 provides the percentages of secure lock screens per country.

The model shows that users in most non-U.S. countries in our sample were between 31 % and 76 % more likely than Americans to have a secure lock screen. Only users in Italy were almost half as likely as U.S. users to secure their devices this way. This clearly shows that the level of protection for data on a smartphone is considerably different between countries. The model also suggests that the older a user gets, the less likely he or she is to have a secure lock screen. Among the genders, male respondents were 38 % more likely to have a secure lock screen, whereas the strongest effect came from those unwilling to disclose their genders: they were 178 % more likely. This result is intuitive: those exhibiting privacy-preserving behaviors while taking our survey also exhibit privacy-preserving behaviors in their use of smartphones.

Reasons for (Not) Having a Secure Lock Screen

The remainder of our analysis is based on the first 8,000 users who completed the full survey. Age and gender demographics showed similar biases for this subgroup, so we will continue to control for these effects. The most frequently occurring codes used to broadly categorize the open-ended responses in question 2 are outlined in Table 2. The table also shows which categories had significant omnibus differences in counts between countries. Looking at the significant differences in detail, we built logistic regression models for each of them with the U.S. as the reference case. Table gives an overview of the results and includes only effect sizes for those models where country had a significant main effect and the individual country estimate was significantly different from 0 ($p < .05$).

The data shows that reasons for having a secure lock screen differ considerably between countries. For example, while Australian users did not differ at all from the U.S. reference group, participants in the Netherlands were 40 % less likely to mention a particular protection scenario, such as losing a phone or having it stolen. Similarly, participants in Italy or Japan are 77 % and 91 % more likely to mention an action – such as unwanted use, someone making calls, or abusing social media accounts – that they want to protect themselves from. German participants appear to think in a goal-oriented fashion about smartphone protection: they were 40 % more likely to mention protection goals and more than 4.5 times as likely to refer to the importance of protection.

Secure Unlock Responses		
1. Given protection goal	1,629	*
2. Protect against attacker (e. g. friends, children, thieves)	1,004	
3. Protect information	658	*
4. Protect from scenario	629	*
5. Protect certain action (e. g. calls, app use)	304	*
6. Lock is mandatory/recommended	105	*
7. Emotional reasons/sentiments	99	
8. Protection is necessary in general	47	*
9. Other reasons/don't know	215	
Slide-to-Unlock Responses		
1. Inconvenience	1,795	*
2. Absence of threat	1,340	*
3. Carelessness	381	*
4. Conflict with usage pattern	176	*
5. Protect using another measure	171	
6. Not secure anyway	90	*
7. Other reason/don't know	185	

Table 2. Major codebook categories and how many respondents mentioned them in total. An * denotes a significant omnibus difference in counts for each category between countries (Chi-square test, $p < .05$).

Looking at the reasons for not having a secure lock screen, the differences are not quite as differentiated. Most countries, especially non-English speaking ones, more frequently mentioned inconvenience and lock screens not being secure anyway; they less often referred to the absence of a threat and not having thought about the subject. It is interesting to note that Canadian users did not differ at all from the U.S. reference group in the reasons they gave within our sample; respondents from the UK differed only by referring to the absence of a threat less frequently. Also, Japanese users were five times more likely to consider using a secure lock screen to be inconvenient.

Data Sensitivity

To elucidate the influence of perceived sensitivity as a proxy for protection intention, we conducted an ANCOVA on the 7-point scale responses to question 3, using country and survey group (SU vs. StU) as independent variables, with age and gender as covariates. We found significant main effects for country ($F_{7,7984} = 55.3$, $p < .0001$, generalized $\eta^2 = .046$) and survey ($F_{1,7984} = 990.9$, $p < .0001$, generalized $\eta^2 = .110$), and a significant interaction between the two variables ($F_{7,7984} = 6.14$, $p < .0001$, generalized $\eta^2 = .005$).

Table 4 provides an overview of the results. The interaction is not disordinal, and its effect size is very small. We will thus also inspect main effects directly. As expected, users with a secure lock screen score much higher (4.54, $sd = 1.56$) than their unprotected counterparts (3.44, $sd = 1.60$) overall. Looking at countries, pairwise Holm-corrected post-hoc

	Reason for having a secure LS (SU group)									Reason to not have a secure LS (StU group)						
Code number	1	2	3	4	5	6	7	8	9	1	2	3	4	5	6	7
Australia										1.42	0.77				3.72	
Canada	1.36															
Germany	1.40							4.63		2.34	0.51	0.51			4.07	
Italy	1.65				1.77	0.30				2.46	0.53	0.41			7.62	
Japan	1.29		0.53		1.91	0.30				5.07	0.33	0.35				
Netherlands			0.49	0.60						2.84	0.37	0.59			7.62	
UK	1.30					0.43					0.60					
Overall Count	1,629	1,004	658	629	304	105	99	47	215	1,795	1,340	381	176	171	90	185

Table 3. Significant odds ratios for major codebook categories by country. Code numbers can be found in Table 2. Values are derived from a logistic regression model that compensated for age and gender differences.

Country	% Secure	StU-Sensitivity	SU-Sensitivity	Δ-S
Australia	72.6	3.28 (1.53)	4.53 (1.57)	1.25
Canada	70.9	2.95 (1.48)	4.28 (1.59)	1.33
Germany	73.5	3.46 (1.45)	4.39 (1.54)	0.92
Italy	50.4	3.61 (1.50)	4.75 (1.52)	1.13
Japan	66.2	4.46 (1.66)	5.16 (1.48)	0.70
Netherlands	70.5	3.28 (1.50)	4.20 (1.53)	0.91
UK	76.4	3.31 (1.65)	4.46 (1.58)	1.15
United States	64.6	3.17 (1.56)	4.56 (1.49)	1.40
Overall	68.0	3.44 (1.60)	4.54 (1.56)	1.10

Table 4. For each country: (a) percentage of users with secure lock screens (screener, $N = 21,451$), (b) mean sensitivity scores and *sd* of those in the StU group, (c) those in the SU group, (d) the difference between (b) and (c) ($N = 8,000$).

t-tests show that Japanese respondents consider the contents of their smartphone to be much more sensitive than other countries. To a lesser extent, this is also true for users in Italy. In terms of the interaction effect, the table shows that the distance between the means of the SU and StU groups varies and is smaller for the non-English speaking countries, suggesting that having a lock screen may be less of a security concern, and more of a usability concern in these countries, or mirroring the findings from question two.

DISCUSSION

Our results provide a wider view on issues discussed in previous studies [5, 6, 11]. Most notably, we find that using a more diverse sample in terms of nationalities, inconvenience and protecting against specific attackers are more common concerns than previously reported [6].

Furthermore, demographic differences (e.g., nationality and age) should be taken into account when designing authentication systems for smartphones. For instance, older users were significantly less likely to use a secure lock screen. This indicates that current approaches might be less appropriate for older populations, and special efforts should be made to make security mechanisms appealing to these users. This is especially apparent for the Japanese participants, who were generally older: they reported inconvenience significantly more often than participants from the other countries in our study. This is even worse (and more surprising) considering that Japanese respondents rated the data on their devices as most sensitive within participants of our study. An important next step in this line of work is thus to create individual interventions based on the exhibited motivations within each country, to try and increase the adoption of secure lock screens.

Our results also show that despite differences between countries, inconvenience is a major driver across all countries that keeps people from using secure lock screens. Assuming that current authentication systems like PINs and pattern locks have good usability properties [11], this means that users are very likely to reject any systems that are less convenient or slower (or are simply perceived to be). One way to reduce this risk is minimizing the numbers of required authentications throughout the day [7]. Recent work on biometrics for smartphones showed that a well-designed and convenient/fun system can get people to use secure locks [3].

Due to the use of GCS for Android, our results are automatically limited to a certain user base, i.e., users of Android smartphones. That is, we can not compare to users of other platforms, which often show different privacy and security attitudes [2]. Nonetheless, we believe that the differences that we identified provide interesting cross-national insights that will inform further development of smartphone authentication systems.

Finally, we did not design our study to shed light on what causes these differences. While this needs to be the subject of future work, we speculate that aspects of culture and history play an important role. The most notable differences we found occurred for the non-English speaking countries in our sample. Furthermore, the one culture that can be considered non-Western also deviated from the general pattern of the results most strongly. We believe that this provides clear evidence that we can leverage the different reasons for not having a lock screen to provide more convincing arguments to users. For example, nudges that refer to possible threats to users' privacy could be more effective in European countries, where users appear to be more worried about threats to their data.

ACKNOWLEDGEMENTS

This work was supported by the FITweltweit program of the German Academic Exchange Service (DAAD), the Intel Science and Technology Center for Secure Computing, and the U.S. National Science Foundation under awards CNS-1318680 and CNS-1528070. We would like to thank Jethro Beekman, Francesco Bombassei, Lauren Carrozza, Nicholas Christin, Eiji Hayashi, Adelina Iacob, Tim van Kasteren, Kegan Kawamura, Bart Knijnenburg, Matteo Miraz, Kanako Neale, Allison Newell, Yumi Oishi, Gala Garcia Prieto, Madhu Reddy, Gabriele Scodellaro, Conny Veerman, and Jeroen van Velden.

REFERENCES

1. Dorothée Behr. 2015. Translating Answers to Open-ended Survey Questions in Cross-cultural Research: A Case Study on the Interplay between Translation, Coding, and Analysis. *Field Methods* 27, 3 (August 2015), 284–299. DOI: http://dx.doi.org/10.1177/1525822X14553175

2. Zinaida Benenson, Freya Gassmann, and Lena Reinfelder. 2013. Android and iOS Users' Differences Concerning Security and Privacy. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13)*. ACM, New York, NY, USA, 817–822. DOI: http://dx.doi.org/10.1145/2468356.2468502

3. Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 1411–1414. DOI: http://dx.doi.org/10.1145/2702123.2702141

4. Tamara Dinev, Massimo Bellotto, Paul Hart, Vincenzo Russo, Ilaria Serra, and Christian Colautti. 2006. Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management* 14, 4 (2006), 57. DOI: http://dx.doi.org/10.4018/jgim.2006100103

5. Serge Egelman, Sakshi Jain, Rebecca S. Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. 2014. Are You Ready to Lock? Understanding user motivations for smartphone locking behaviors. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*. ACM, New York, NY, USA, 750–761. DOI: http://dx.doi.org/10.1145/2660267.2660273

6. Marian Harbach, Emanuel von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception. In *Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 213–230. https://www.usenix.org/conference/soups2014/proceedings/presentation/harbach

7. Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. 2013. CASA: Context-aware Scalable Authentication. In *Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS '13)*. ACM, New York, NY, USA, Article 3, 10 pages. DOI: http://dx.doi.org/10.1145/2501604.2501607

8. Lawrence L. Kupper and Kerry B. Hafner. 1989. On Assessing Interrater Agreement for Multiple Attribute Responses. *Biometrics* 45, 3 (1989), pp. 957–967. http://www.jstor.org/stable/2531695

9. Paul McDonald, Matt Mohebbi, and Brett Slatkin. last access: 09/07/2015. Comparing Google Consumer Surveys to Existing Probability and Non-Probability Based Internet Surveys. Retrieved from http://www.google.com/insights/consumersurveys/static/consumer_surveys_whitepaper.pdf. (last access: 09/07/2015).

10. Susan Rose, Nigel Spinks, and Ana Isabel Canhoto. 2014. *Management Research: Applying the Principles*. Routledge, New York, NY, Chapter Supplement: Quantitative Content Analysis, 117–126.

11. Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the Wild: A Field Study of the Usability of Pattern and Pin-based Authentication on Mobile Devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (MobileHCI '13)*. ACM, New York, NY, USA, 261–270. DOI: http://dx.doi.org/10.1145/2493190.2493231