Analysis of Application Navigation Methods using Card Sorting

Pranav Sarma Venkatramanan
Rochester Institute of Technology
Rochester, NY, USA
ps4554@rit.edu

ABSTRACT

With the continuous exponential development in mobile device technology, one thing that has become a worrisome factor is how secure the devices are and if given the opportunity to configure those security settings by themselves, will the user find it easy or tough. Hence with this in mind, in this paper I have briefed how HCI is an important aspect to improve mobile device security from a user's end and how proper research implementations can improve the usability usage of security tools in mobile devices. The studies I had conducted involved on capturing the actions of users while they navigate through the categories of a fictional app involving security configuration, using a UI design technique called as Card Sorting. This was done to gauge the user's UI mental model and use it to design the app's navigation. With the data collected from the studies, it was found that users though having vastly different UI expectations, they would still be able to adapt to a UI built on common themes from the study about 80
Copy to clipboard

Author Keywords

Authors' choice; of terms; separated; by semicolons; include commas, within terms only; this section is required.

CCS Concepts

•**Security and privacy → Usability in security and privacy;** Please use the 2012 Classifiers and see this link to embed them in the text: https://dl.acm.org/ccs/ccs_flat.cfm

INTRODUCTION

Mobile technology is one which is used in portable devices to establish communication of data between the necessary parties. Over the years, it has exponentially improved beyond comprehension, compared to how it was estimated to when first introduced. Almost within these 2 decades, a simple pager for 2 way text messaging has now went on to transform into smart phones and laptops capable of performing long distance phone calls, video calls, multimedia messages, internet browsing and to making professional cinema documentaries using its camera. Rather than commuting to a place to access something, the humble modern day mobile devices have brought everything under a user's finger tips. Paying the telephone electricity bills? Check. Transferring money to another account? Check. Ordering food, booking a flight ticket, shopping a product, reading a book, watching live TV, playing online games, working remotely from home? Every one of them is taken care of by these devices.

One thing which also needs equal importance with the development of such technologies in today's world is the security aspect associated with them. With the advent of mobile technology, the manner in which data is requested, shared and stored has been revolutionised. Your personal information, internet browsing activities, chats, voice calls and every other data found in your devices which use mobile technology, if went unprotected could end up in the hands of adversaries. This misuse of your data located in mobile devices or of the mobile devices themselves with the intent to harm someone is generally termed as Cybercrime. Monetary loss due to cybercrime overall leads to more than billions of dollars, which tells about the scale of damage it can cause once afflicted and how important is the role of mobile device security in mitigating this factor.

Cybercrime attacks generally happen by exploiting the loopholes and weakness of security in mobile devices. This can be generally found in various target points like software, hardware, networks and also from the user's lack of awareness itself. Despite the various fixes patches made to possibly counter them, as mobile technology keeps updating, so do the type of methods tools to attack vulnerable mobile devices. Even though fixing and patching done by the corresponding service providers keep the system safe to a level, users also do need to fix issues from their end to close all options for possible attacks- the most popular ones include having an old or no password, blindly granting permission/cookie controls and divulging sensitive data to strangers on urgent or polite requests.

While the above mentioned situations could be addresses and possibly solved via proper awareness programs, the user would still need to know on what how to configure the customisable security settings in their mobile devices in order to secure them even better and however they want to. Though the WHAT

CHI'20, April 25–30, 2020, Honolulu, HI, USA

ISBN 978-1-4503-6708-0/20/04...$15.00
DOI: https://doi.org/10.1145/3313831.XXXXXXX

factor can again be covered by having various awareness initiatives, in terms of the HOW factor most OS designs are generally complained as being less user friendly in terms of configuring security related settings in the devices. This is mainly due to the variation of perspectives with respect to app navigation between the developers and the users. The developers, since they are the ones who have constructed the technology, have the undue advantage of already knowing its layout and would not be able to recreate the same navigation experience as exactly as a user would during the testing process. Because of this reason, the usability factor of the technology gets affected in the end and to counter this, proper tests with users need to be conducted by developers on the technology as early as during the design process itself to save the overall cost and time involved in developing and deploying them. By this, users will be able to find issues with respect to structuring in the technology, which would not have been noticed by developers.

This study of observing how users interact with different computer technologies is called Human-Computer Interaction (HCI). Researchers and developers use this study mostly to observe the reaction of users when they operate a software/application, figure out their mental models and use it to align its design accordingly. Here, a mental model is defined as the representation of a user's thought process, muscle memory and behaviour while using the software/application. The best HCI design is the one which is considered the most usable by all

In recent times a lot of UI/UX techniques have been created and studied to enhance the usability factor of software/applications for users. One of them is Card sorting, which is tested on group of participants to generate an analysis of their mental models. Most commonly, this technique is used in designing a navigation structure for applications and operating software. It is done by providing a list of categories to the participants in the form of cards, which are needed to be sorted together into groups based on their commonalities or left separately, however required by them.

The 2 sub types of car sorting which I will use in my study are the Open card and Closed card sorting. Open card sorting is the sub technique of Card sorting, where the participants can create their own groups and sort the presented cards under them, based on the commonalities which they find from their perspectives. Closed card sorting is where participants are made to sort the cards in the groups given by the organiser only, based on the commonalities they find in the given groups with the presented cards

In this paper, I will create a mental model analysis using both the above Card sorting techniques for the navigation of a fictional security configuration app having various security based features as its categories. Since I am conducting this study remotely, I will be using an online software called Optimal workshop which helps in conducting card sorting study online, documents the answers with also providing basic level analysis and graphs

RELATED WORK

I was mainly inspired by the non-usability of mobile devices with regards to their security configuration, especially mobile phones. Even if lot of users become aware of the unwanted configurations, they find it hard to navigate to the proper place where it can be done. Moreover, there are too many options to choose from and with lesser insight on why they are required. Research has been going on for bringing all of these under a separate privacy application and to include better features to control the configuration easily [CMU paper]. Hence I wanted to test how users would want the setup of such an application to be, if given a list of features which I would create.

Basics on Mobile device security include [19] [2] [11] [6] [20] [9] [15] [14] [22]

Important frameworks include [1] [25] [18] [16] [21] [24] [4] [27] [23] [10] [28] [5]

Other frameworks include [30] [13] [26] [8] [29] [17] [3] [7] [12]

RESEARCH QUESTIONS

1. **Do participants have a common mental model to navigate an application?**
2. **Will the users be able to adapt to a different navigation model?**
3. **Is it possible to create a universal app navigation structure?**

RESEARCH PLAN

My study will be done using the Card sorting, which is a UI technique used to design information architecture (IA), workflows, menu structure, or web site navigation paths. The test's organiser first identifies the key features of the test's research topic and writes them down over physical cards. The test's participants are then made to sort the given cards with respect to how they see the commonalities between them. The cards can be sorted either into groups or left as individuals.

I will be conducting this study online using the Optimal Workshop software. It is an online IT service based software which helps in conducting tests like Card sorting online and present results in both quantitative and pictorial formats

First, I will prepare list of features which my app will support and think of proper names for them. These are the categories which will be used as cards for the sorting. Once that is done, I shall upload all those details in the software. Then after getting my participant's willingness in this study, I shall explain them about my study, working of each feature present in the card labels and how to perform the test in the software. After then, I shall be giving them at least a day's time for my participants to grasp the study and ask any queries.

Once they are ready, I shall conduct my first study- Open card sorting- where the cards will be shuffled presented to the participants. The participants will have to sort the cards into groups which they will create, based on the commonalities they find between those set of sorted cards. This is done to see how users would naturally like to structure the cards based on the common features they find from their perspectives. Once that is done, I will analyse and come up with (i) The average number of groups created (ii) The possible commonalities between the cards which each user saw while sorting them into the same group and (iii) The similarities between each user in terms of groups and the commonly sorted cards. With this study, I will be able to see how much the mental model of my participants vary between each other and be able to conduct my second study

With the results from my analysis in the first study, I will then conduct my second study- Closed card sorting- where cards will again be shuffled and presented to participants. But now, these same participants will have to sort them only into the groups which I had created, based on the analysis of the first study's results. Moreover, I had also made my own sorted list of cards and the groups they would come under, again based on the analysis of the first study's results for my reference. This study is done to test whether despite different perspectives in card sorting, will all the participants be able to sort properly in given set of groups as per my reference list. Once the study is done, I shall analyse if users were able to sort them exactly as I sorted for my reference. With this I can find out if users would be able to adapt themselves to a slightly different and more universal mental model.

METHODOLOGY

Participants

I had conducted a total of 2 evaluations which had the same 5 participants, aged around 24-26 who are good users of smartphones and have a beginner level of knowledge with respect to privacy and security of data and devices. Once they had agreed to participate after I gave an overview on the study, they were then given a brief description on the Card sorting technique, how to perform it in the Optical Workshop software and the explanation for each of the app's categories which features as the cards for the study.

Cards

Both the evaluations were heuristic ones based on open card closed card sorting techniques, where users are given set of 19 cards specifying the features my personalised privacy app will provide. These 19 were selected based on the default features used by various popular security related apps for mobile devices:

- **Custom AdBlock Manager:** Has 3 levels of Ad blocking: Essential (blocks disruptive ads like pop-ups, banners, autoplay videos, etc which violate acceptable ad standards), Balanced(blocks most of ads, especially disruptive ones) , Strict (blocks almost all ads)

- **App based AdBlock usage:** Helps in users customising which apps need to/need not be blocked from disruptive/non-disruptive ads

- **Threat scanner:** Helps in scanning for all kinds of malware

- **Disk space booster:** Helps in clearing cache/browsing history/cookies

- **Disk space analyser:** Display's the amount of data, data format and files in phone's folders. Also able to identify duplicate data

- **Custom Disk Space Booster:** Helps in customising the kind of data to be cleared from device

- **Software update reminder:** Helps in giving latest updates of apps software along with mentioning an urgency level of 1-100

- **Phone tool analyser:** Helps in displaying analytically about what all apps use phone tools like Phone log, Contact, Calendar, Camera, Location, Speaker, Mic, SMS, Battery in real time.

- **Phone tool Identifier:** Helps in identifying alerting based on Phone tool analyser's data, if tools are activated by apps even when they are not being used

- **Phone tool manager:** Helps in configuring what all apps can use what all phone tools

- **VPN:** Helps in activating VPN based on user's preferences

- **App and Internet data analyser:** Helps in analysing amount of data amount of time apps are used per day/week/month

- **App and Internet data controller:** Helps in controlling amount of data amount of time apps are used per day/week/month

- **Password manager:** Helps in saving, regularly updating and keeping passwords safe. Also helps user make better decisions related to passwords

- **App/File locker:** Helps in giving extra level of authentication to certain apps/lockers

- **Storage locker:** Helps in giving extra level of authentication to phone storage

- **Storage backup:** Helps in giving another level of backup to phone storage

- **Theft manager:** Captures last known location, takes photo and tracks their activity logs after an alarm is triggered from your side. Also deletes all data from device after few wrong authentications

- **Manage other devices:** Helps in managing and monitoring other devices of joint accounts, especially users having kids with mobile devices and who's account is joined with yours

All 5 participants agreed that names of features corresponding functionalities were easy to understand and recollect. Once that was confirmed, the participants were made to perform the study

Working

In both the Card sorting techniques, the virtual cards were shuffled by the software and presented to users in the left panel. The participant will have to press the left button on the card, drag it to the right panel and drop it.

In the open card sorting technique, the right panel will be empty. Once the card from the left panel is dropped to the right, the card would arrange itself in order. Once dropped in the right panel, regardless if the other cards will be grouped with it or left as an individual card till the end, the participant will have to enter the group label they find as apt for its working feature. In this process, if a card needs to be sorted with another one found in the right panel, the participant will have to drag the card from left panel and drop it over the card it wants to group together with.

In the closed card sorting technique, the only difference is that the right panel will already have groups with labels on them. The participants will not be able to create new groups on their own and will have to only drag the cards and drop them in the group which they find relatable

RESULTS

RESULTS OF FIRST STUDY

In this fashion, my participants sorted all 19 cards by themselves according to the understanding of their mental models. This type of study was mainly done to analyse the individual perspectives of the participants with respect to sorting cards based on its commonalities

From this study, Participant 1 had sorted all cards into 4 groups as given: (i)AdBlock Manager: App based AdBlock usage, Custom AdBlock Manager

(ii)Device Manager: Software update reminder,Phone tool manager, Phone tool analyser, Phone tool identifier, App and Internet data controller, App and Internet data analyser, Manage other devices

(iii)Security: Password manager,Theft manager,VPN,App/File locker,Threat scanner

(iv)Storage: Storage locker,Storage backup,Custom Disk Space Booster,Disk space analyzer,Disk space booster

From this study, Participant 2 had sorted all cards into 4 groups as given:

(i)AdBlock: Custom AdBlock Manager, App based AdBlock usage

(ii)Defender: Threat scanner

(iii)Smart Clean: Disk space analyzer, Disk space booster, Custom Disk Space Booster

(iv)Smart Data Control: App and Internet data analyser, App and Internet data controller

(iv)Tool Manager: Phone tool manager Phone tool identifier Phone tool analyser

(v)Updates: Software update reminder

(vi)Vault: App/File locker Password manager Storage locker Storage backup Theft manager Manage other devices VPN1 VPN

From this study, Participant 3 had sorted all cards into 4 groups as given:

(I)Phone manager/analysers: Phone tool identifier Phone tool manager Password manager Phone tool analyser App and Internet data analyser App/File locker App and Internet data controller

(ii)Security updates/notification: Theft manager Software update reminder Threat scanner App based AdBlock usage Custom AdBlock Manager

(iii)Storage: Disk space booster Disk space analyzer Storage locker Storage backup Custom Disk Space Booster

(iv)Vpn: VPN Manage other devices

From this study, Participant 4 had sorted all cards into 10 groups as given:

(i)AdBlock: App based AdBlock usage Custom AdBlock Manager

(ii)App and Internet data: App and Internet data analyser App and Internet data controller

(iii)App Locker/Password: App/File locker Password manager Theft manager

(iv)Disk space: Disk space booster Disk space analyzer Custom Disk Space Booster

(v)Manage other devices: Manage other devices

(vi)Phone tool: Phone tool identifier Phone tool manager Phone tool analyser

(vii)Software update reminder: Software update reminder

(viii)Storage: Storage locker Storage backup

(ix)Threat scanner: Threat scanner

(x)VPN: VPN

From this study, Participant 5 had sorted all cards into 8 groups as given:

AdBlock: App based AdBlock usage Custom AdBlock Manager

Data Analyser: App and Internet data analyser App and Internet data controller

Disk space: Disk space analyzer Disk space booster Custom Disk Space Booster

External Security Measures: Threat scanner Theft manager

Internal Security Measures: App/File locker Storage locker Storage backup Password manager

Other: Manage other devices Software update reminder VPN

Phone tools: Phone tool identifier Phone tool analyser Phone tool manager

From the above study, the average numbers of groups created were 6.8 7. The groups which were most commonly created by the participants include the Adblock manager, Device manager/Tool manager, Locker/Vault/Security, Memory manager/Disk space/Smart clean, VPN and Manage other devices/Others. The Adblock manager groups were commonly found to have 2 of the Ad blocking features, The Device manager/Tool manager groups were found to commonly have the 3 Phone tool features, the Locker/Vault/Security groups were found to commonly have the 2 Storage based features and the App/File locker feature, the Memory manager/Disk space/Smart clean groups commonly had the 3 Disk space related features, VPN groups had the lone VPN feature and the Manage other devices/Others groups commonly had the Manage other devices Software update reminder features. Hence it is now clear that few of my participants have similar mental models while others have varying mental models

ANALYSIS FROM THE FIRST STUDY

The analysis I am planning to do based on the first study include (i) the average number of groups created (ii) The possible commonalities between the cards which each user saw while sorting them into the same group and (iii) The similarities between each user in terms of groups and the commonly sorted cards

Keeping in mind of the results from my first study mentioned just before, I created 7 groups, labelled their names based on the common set of groups created labelled by the participants themselves and also sorted the 19 cards according to the groups they would likely fit, also as per how most of the participants had sorted the cards

Here is my sorted list:

(I) Adblock: App based adblock, Custom Adblock (ii) Tool manager: home tool manager, identifier analyser (iii) Locker: Storage locker, storage backup, app/file locker (iv) Memory: Disk space booster, analyser, custom booster (v) Defender: Threat scanner and manager (vi)Internet: App internet analyser and controller (vii)Others: Software update reminder, manage other device, VPN

RESULTS OF SECOND STUDY

In the second closed card sorting technique, my participants were made to sort all cards within 7 groups I had decided based on the first study. I had not divulged as to how I would have sorted them, in order to confirm if the all the participants who naturally seem to have different mental models (as seen in the analysis of first study) would be able to sort cards as I did. From this study, it was found out that Participant 1 had sorted 15/19 cards correctly (78.9473 percent correct), Participant 2 sorted 16/19 correctly (84.2105 percent correct), Participant 3 sorted 12/19 cards correctly (63.1578 percent correct), Participant 4 sorted 17/19 cards correctly (89.4736 percent correct) and Participant 5 sorted 16/19 cards correctly (84.2105 percent correct). On an average, all participants correctly sorted 80 percent of cards. Hence a participant would be more than likely to adapt themselves to a slightly different but possibly universal mental model

INTERPRETATION

From my results, I see that despite users being in the same age group and almost the same knowledge level in device security, they have different opinions with regards to how an app needs to be designed with respect to its features usability. We have read how each had created varying number of groups from 4 to 10 and averaging around 6.8   7. Also despite the fact that they have different opinions to it, if they are brought to a common field, would on an average of 80 percent of the time correctly sort the cards into the groups I had created for them to be sorted in. I will have to now reframe my original structure based on the new results and possibly try out the test again if required

CRITICAL REFLECTION

From the overall results, I believe that the technique of doing both kinds of card sorting techniques will be a good primary assessment before starting to design the structure of the app, which can adapt to the mental model of all the participants. From the first study I was able to gain the pulse of the mental models of my participants to use to my advantage of designing the app's navigation structure in the second study. Moreover from the second study, I can confirm if my analysis is right, else if not I can reframe the navigation structure more finely to get the perfect version of it

CONCLUSIONS

From the overall results, I believe that the technique of doing both kinds of card sorting techniques will be a good primary assessment before starting to design any app. From the first open card sorting, I got to know the range of different mental models my participants have. After this I started on building on my own initial groups, having the most common features mentioned as per the results from this study. With the second closed cart sort study, I was able to verify if my designed set of group and its features will be usable compatible enough for my same set of users. Furthermore, from that result, I might try to again create a new set of groups in necessary but will definitely change how the features have been sorted under my created groups. With this, I would be able to design my app interface properly without the fear of whether it will be compatible with users or not, with respect to usability.

LIMITATIONS AND FUTURE WORK

As we have seen till now, even though the results reflect on how the advantages of involving users right from the start of app designing could be really helpful in improving its usability factor and how card sorting technique can be a reliable tool to support the structuring of an application's features, the number of participants and results need to be even of even higher number and diverse enough for this kind of experiment compared to mine, in order to properly reflect the real world scenario.

If an app needs to be truly usable for users, the designers should consider more number of diverse users compared to how I did hence get the proper data and understand their mental models, so as to design it as perfectly usable as possible. But also, I feel that too many diverse users would mean too much data to aggregate and come to a common ground, which I feel would not be practical and lead to lot of confusion and time to finish the study. Hence more research is needed on finding out the balanced number of participants required

I am also afraid that if I had brought in a 3rd Closed Card sorting study by analysing both the results of the 1st and 2nd ones, the participants might possibly change their entries this time compared to their previous entries due to rethinking of their actions. Anyway, I will have to perform that 3rd study in order to find out the practical results

ACKNOWLEDGMENTS

Add any acknowledgements here...

REFERENCES

[1] Rebecca Balebako, Pedro G Leon, Hazim Almuhimedi, Patrick Gage Kelley, Jonathan Mugan, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Nudging users towards privacy on mobile devices. In *Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*, pages 193–201. Citeseer, 2011.

[2] Michael Becher, Felix C Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf. Mobibecher2011mobilele security catching up? revealing the nuts and bolts of the security of mobile devices. In *2011 IEEE Symposium on Security and Privacy*, pages 96–111. IEEE, 2011.

[3] Carolyn Brodie, Clare-Marie Karat, John Karat, and Jinjuan Feng. Usable security and privacy: a case study of developing privacy management tools. In *Proceedings of the 2005 symposium on Usable privacy and security*, pages 35–43, 2005.

[4] Liang Cai and Hao Chen. Touchlogger: Inferring keystrokes on touch screen from smartphone motion. *HotSec*, 11(2011):9, 2011.

[5] Eun Kyoung Choe, Jaeyeon Jung, Bongshin Lee, and Kristie Fisher. Nudging people away from privacy-invasive mobile apps through visual framing. In *IFIP Conference on Human-Computer Interaction*, pages 74–91. Springer, 2013.

[6] Jessica Colnago, Yuanyuan Feng, Tharangini Palanivel, Sarah Pearman, Megan Ung, Alessandro Acquisti, Lorrie Faith Cranor, and Norman Sadeh. Informing the design of a personalized privacy assistant for the internet of things. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[7] Serge Egelman and Eyal Peer. The myth of the average user: Improving privacy and security systems through individualization. In *Proceedings of the 2015 New Security Paradigms Workshop*, pages 16–28, 2015.

[8] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. The influence of friends and experts on privacy decision making in iot scenarios. *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW):1–26, 2018.

[9] Jennifer Evans-Cowley. Planning in the real-time city: The future of mobile technology. *Journal of Planning Literature*, 25(2):136–149, 2010.

[10] Qatrunnada Ismail, Tousif Ahmed, Kelly Caine, Apu Kapadia, and Michael Reiter. To permit or not to permit, that is the usability question: Crowdsourcing mobile apps' privacy permission settings. *Proceedings on Privacy Enhancing Technologies*, 2017(4):119–137, 2017.

[11] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra. A survey on security for mobile devices. *IEEE communications surveys & tutorials*, 15(1):446–471, 2012.

[12] Tuukka Lehtiniemi and Yki Kortesniemi. Can the obstacles to privacy self-management be overcome? exploring the consent intermediary approach. *Big Data & Society*, 4(2):2053951717721935, 2017.

[13] Yuting Liao, Jessica Vitak, Priya Kumar, Michael Zimmer, and Katherine Kritikos. Understanding the role of privacy and trust in intelligent personal assistant adoption. In *International Conference on Information*, pages 102–113. Springer, 2019.

[14] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. To deny, or not to deny: A personalized privacy assistant for mobile app permissions.

[15] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun Aerin Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pages 27–41, 2016.

[16] Changchang Liu, Supriyo Chakraborty, and Prateek Mittal. Deeprotect: Enabling inference-based access control on mobile sensing applications. *arXiv preprint arXiv:1702.06159*, 2017.

[17] Won Hyung Park, Dae Hyeob Kim, Myung Soo Kim, and Neo Park. A study on trend and detection technology for cyber threats in mobile environment. In *2013 International Conference on IT Convergence and Security (ICITCS)*, pages 1–4. IEEE, 2013.

[18] Mr Bhaskar V Patil, Milind J Joshi, and Mr Hanmant N Renushe. A comparative study for performance meas-urement of selected security tools.

[19] Karen P Patten, Mark Harris, et al. The need to address mobile device security in the higher education it curriculum. *Journal of Information Systems Education*, 24(1):41, 2013.

[20] Jan Pennekamp, Martin Henze, and Klaus Wehrle. A survey on the evolution of privacy enforcement on smartphones and the road ahead. *Pervasive and Mobile Computing*, 42:58–76, 2017.

[21] Giuseppe Petracca, Ahmad-Atamli Reineh, Yuqiong Sun, Jens Grossklags, and Trent Jaeger. Aware: Preventing abuse of privacy-sensitive sensors via operation bindings. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 379–396, 2017.

[22] Hannah Quay-de la Vallee, Paige Selby, and Shriram Krishnamurthi. On a (per) mission: Building privacy into the app marketplace. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 63–72, 2016.

[23] Frederic Raber and Antonio Krueger. Towards understanding the influence of personality on mobile app permission settings. In *IFIP Conference on Human-Computer Interaction*, pages 62–82. Springer, 2017.

[24] Amit Kumar Sikder, Hidayet Aksu, and A Selcuk Uluagac. 6thsense: A context-aware sensor-based attack detector for smart devices. In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pages 397–414, 2017.

[25] Alina Stöver, Felix Kretschmer, Christin Cornel, and Karola Marky. Work in progress: How i met my privacy assistant–a user-centric workshop. *Mensch und Computer 2020-Workshopband*, 2020.

[26] Lynn Tsai, Primal Wijesekera, Joel Reardon, Irwin Reyes, Serge Egelman, David Wagner, Nathan Good, and Jung-Wei Chen. Turtle guard: Helping android users apply contextual privacy preferences. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 145–162, 2017.

[27] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J Weitzner, and Nigel Shadbolt. Better the devil you know: Exposing the data sharing practices of smartphone apps. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 5208–5220, 2017.

[28] Xiaolei Wang, Andrea Continella, Yuexiang Yang, Yongzhong He, and Sencun Zhu. Leakdoctor: toward automatically diagnosing privacy leaks in mobile applications. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(1):1–25, 2019.

[29] Primal Wijesekera, Joel Reardon, Irwin Reyes, Lynn Tsai, Jung-Wei Chen, Nathan Good, David Wagner, Konstantin Beznosov, and Serge Egelman. Contextualizing privacy decisions for better prediction (and protection). In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2018.

[30] Dongsong Zhang. Delivery of personalized and adaptive content to mobile devices: a framework and enabling technology. *Communications of the Association for Information Systems*, 12(1):13, 2003.