Usability versus Privacy instead of Usable Privacy

[Google's balancing act between usability and privacy]

Paul Gerber & Melanie Volkamer
Department of Computer Science
Hochschulstrasse 10
D-64289 Darmstadt, Germany
{paul.gerber,melanie.volkamer}@cased.de

Karen Renaud
School of Computer Science
18 Lilybank Gardens
Glasgow, G12 8RZ, UK
karen.renaud@glasgow.ac.uk

ABSTRACT

A smartphone is an indispensible device that also holds a great deal of personal and private data. Contact details, party or holiday photos and emails — all carried around in our pockets and easily lost. On Android, the most widely-used smartphone operating system, access to this data is regulated by permissions. Apps request these permissions at installation, and they ideally only ask for permission to access data they really need to carry out their functions. The user is expected to check, and grant, requested permissions before installing the app. Their privacy can potentially be violated if they fail to check the permissions carefully. In June 2014 Google changed the Android permission screen, perhaps attempting to improve its usability. Does this mean that all is well in the Android eco-system, or was this update a retrograde move? This article discusses the new permission screen and its possible implications for smartphone owner privacy.

Categories and Subject Descriptors

K [**Computing Milieux**]: Miscellaneous; K.4 [**Computers and society**]: [K.4.2 Social Issues]

General Terms

Psychology of security, risk perception, and risk communication; security education and usable security

Keywords

Android permissions, Usable privacy

1. INTRODUCTION

Android mediates application access to different data or functions via a permissions mechanism. Such permissions (around 150 [1, 7]) are allocated by Android to one of three groups:

1. **Normal** — permissions that enable access to resources (i.e. data and or functions) with which the user can be disturbed but not seriously endangered.
2. **Dangerous** — permissions that enable access to resources that may incur costs and/or touch personal information.
3. **Signature/System** — permissions that enable access to system-critical resources. Those permissions cannot be obtained via the normal installation route, i.e. from downloading and installing an app from Google Play Store.

During the Google Play Store installation process, requested permissions are displayed via a so-called *permission screen*. The user has to agree to grant *all* the requested permissions in order to go ahead with installation. If the user refuses, perhaps because permissions are requested that are not deemed necessary to support the app's functionality or because there is insufficient trust in the app provider, the installation has to be aborted. In recent years this approach has been criticised for various reasons. For example, some researchers refer to timing as an issue. The permission screen is first shown *after* the user clicks on the "install" button (Figures 1(a) and (b) illustrate this). The user has already made the decision to install the particular app [13] and might be less likely to abort the installation. Other researchers argue that the naming and descriptions of permissions are very technical and therefore incomprehensible to many users [12, 4]. Furthermore, it seems unrealistic to expect users to learn and remember every single previously granted permission since around 150 permissions are available [1, 7]. Finally, it was noted that developers tend to demand more permissions than strictly required, perhaps in order to simplify the installation process [6, 16].

In June 2014 Google implemented an extensive update of the Play Store and changed the permission screen. Figure 1(a) shows the former (Play Store Version 4.6.17) screen for the "Wetter app". Here, users are confronted with a list of all requested permissions that are categorized as dangerous. To see "normal" permissions the user clicks on "see all". Figures 1(b) and (c) show the new screen used by Play Store Version 4.8.19. The screen in the middle appears immediately after the user clicks "install"; the screen on the right shows the same screen with revealed details. Google has essentially changed the structure, formulations and level of detail in their new implementation.

Google also introduced another permission feature within their Play Store. It can be viewed when the application is first displayed, *before* the user clicks on the "install" button, by scrolling down to the end of the page and then visiting

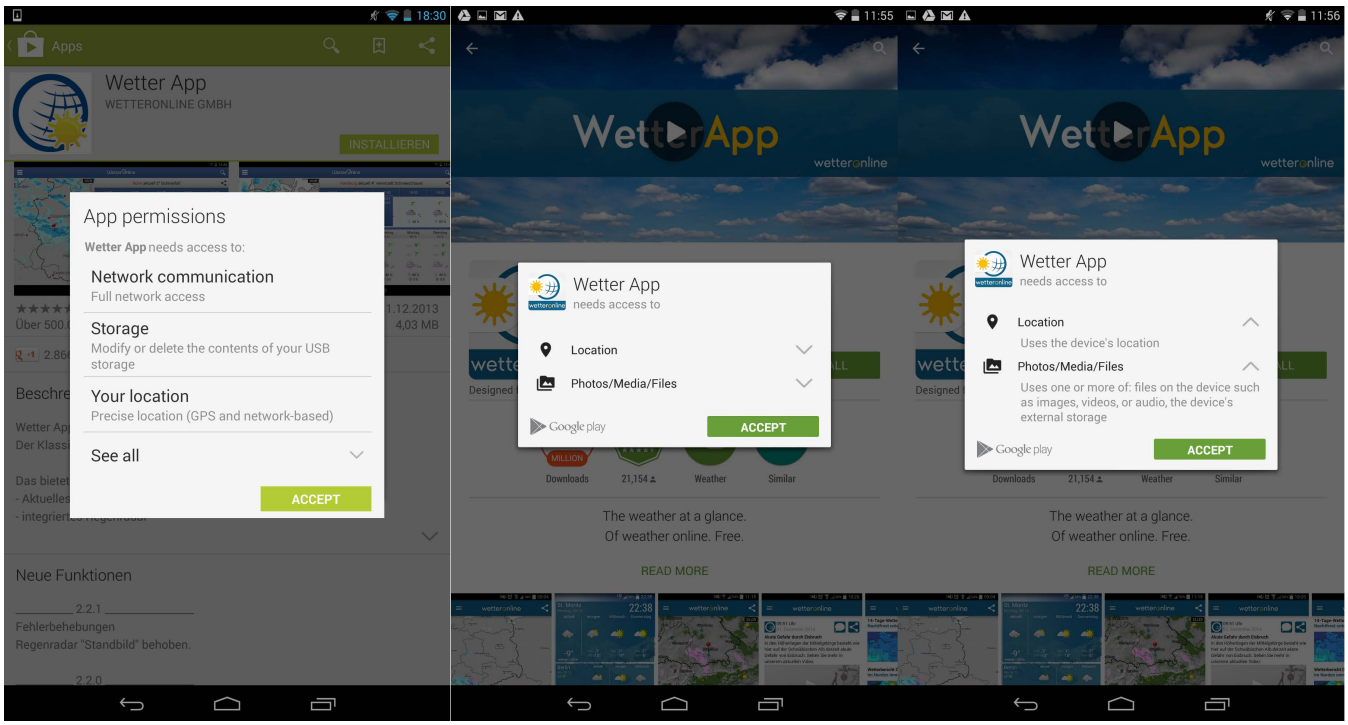

Figure 1: (a) on the left: depiction of permissions of Google Play Store until version 4.6.17 including (b) in the middle: corresponding screen since version 4.8.19 (c) on the right: corresponding screen with revealed details.

the corresponding screen via the note "permission details". Figure 2(a) shows the corresponding screen for the Wetter app[1].

Here we take a critical look at the changes Google has implemented. The focus is currently on possibilities and difficulties the user may experience in protecting their privacy independently, effectively and efficiently. Therefore, we first provide a description of the new permission screen and comment on its characteristics. Thereafter, we investigate the consequences with regard to the user's ability to make decisions about privacy protection. Next, these findings are discussed in the context of current research. The article concludes by outlining a future course of action to improve the current situation.

2. DESCRIPTION OF NEW PERMISSION DISPLAY

Google has refined the "dangerous" permissions, allocating them to one of 13 groups. These are described in some detail in Google's online documentation [9]. When users click on the "install" button they now only see the *groups* to which the requested permissions belong (Figure 1(b)), rather than the permissions themselves. Actual permissions are not displayed, nor does any description thereof appear. Next to each group there is an arrow symbol. By clicking on it, a more detailed description of the respective permission group can be viewed. This description does not, unfortunately, contain a complete list of the requested permissions making up this group (Figure 1(c)).

[1]Wetter is German for weather.

There is no longer a "see all" button. The user cannot easily obtain a complete list of all requested permissions, regardless of whether they are judged "dangerous" or "normal". Furthermore, at this point only twelve groups of permissions are shown. The 13th, called "Other", can only be found in a separate depiction (compare figure 2(a)), which also contains the complete list of these permissions. The user still only has one choice: either agree to grant all permissions and install, or abandon the respective app.

On top of this, with the new permission system Google has also adapted underlying concepts to the core concept of the new groups. In the new implementation, accepting the requested permissions implies an agreement to the entire group of permissions. This means that an app which was previously given only read access to USB storage during installation (therefore the group "photos/media/data" as listed) could upgrade to write permission without prompting the user for this escalation in permissions. Direct user interaction is only needed while requesting a new permission group or a new permission out of the 13^{th} group 'Other'.

3. IMPACT ON PRIVACY PROTECTION

In this section, we propose and discuss potential privacy-related consequences that result from the changes described in the previous section.

3.1 Complicated access to actual permissions

Google's Play Store does not contain any content-related description of the groups. In the more detailed display (Figure 2(a)) there is a link to the online documentation at the

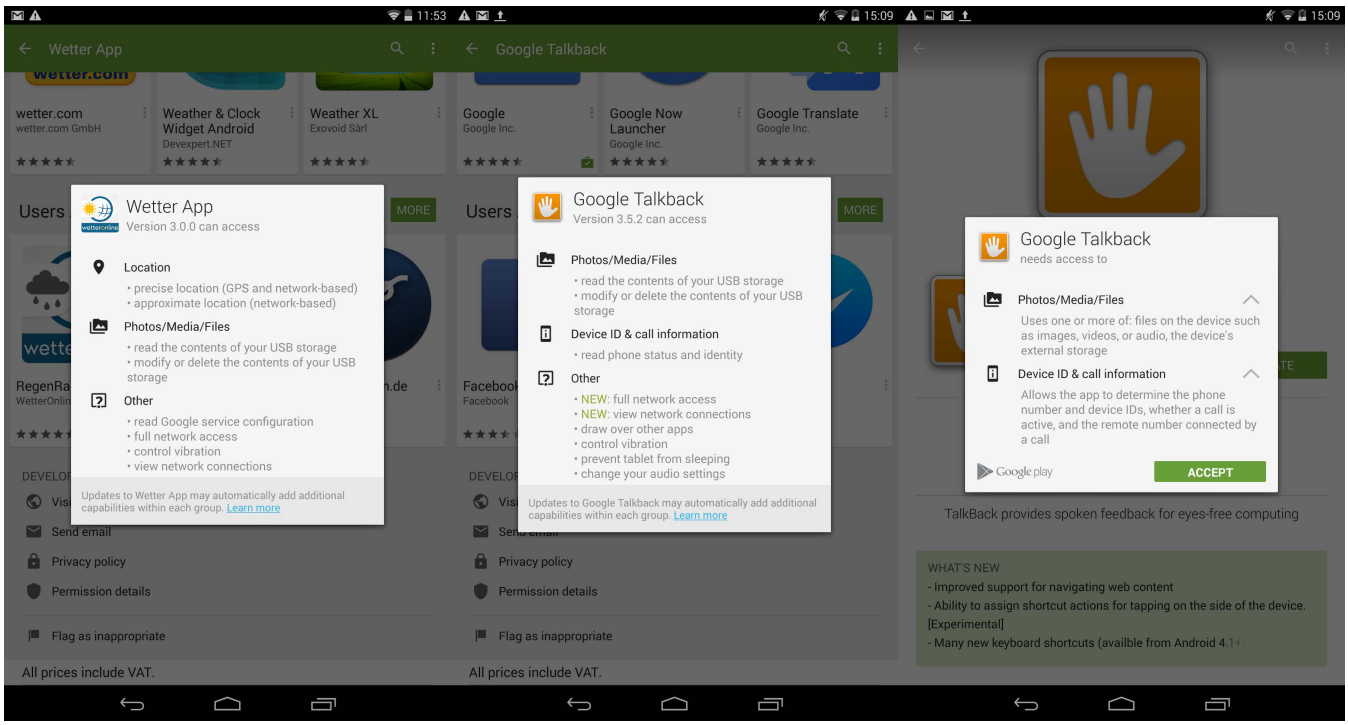

Figure 2: (a) on the left: depiction of the permissions of the app "Wetter app" since version 4.8.19 via "permission details" Play Store. (b) in the middle: depiction which is found under "permission detail" while an app update with additional requested permissions is pending. (c) analogous to (b), but just after clicking the "update" button right on the top of the app-detail-page.

lower edge. This documentation provides information about groups, permissions contained within groups and generally gain insight into the requested permissions. A complete list of all requested permissions can no longer be found in the usual place (i.e. on the permission screen which appears after clicking "install"). This list can only be found via the above-mentioned and newly implemented second permission screen.

Both changes complicate access which probably explains why even an interested and motivated user might lose interest in checking permissions both when installing an app and when it is updated. Privacy protection in the fast-moving Android eco-system turns out to be a Sisyphean task.

3.2 Permission Group Agreement

The fact that an app with permissions belonging to an already-granted group may extend their access to any other permission within the same group (without informing the user) can only be found in the detailed page (see Figure 2(b): "Learn more" link). This means that an app can gain considerably more access without the user's knowledge as long as it remains within the approved permission groups. Thus, with each update, the user's privacy might be increasingly violated without their realising it.

3.3 Complicated access to Additional Permissions at Update

If Android demands manual intervention by the user, he/she has to visit the corresponding app-detail-page in the Play Store and manually "update" in order to confirm the update and implicitly also the new set of permissions. After this once again the permission screen is shown and the user can agree to the update, or not as the case may be. As Figure 2(c) shows (in comparison to Figure 2(b)), the user is not able to check the updated permissions, because the category "Other" is not shown on the permission screen. The user does not see which permissions he is actually granting. Only in the "permission details" which are reachable via a link at the end of the app-detail page, is this listed with a green "new" (Figure 2(b)).

If the user trusts Google's statement that he will always be asked to check and confirm changes in the "Other" group, and no such changes are highlighted, he/she will probably not seek further detail. The same applies to a user who did not read the documentation at all, and therefore in all probability does not even know about the existence of the group since it never appears on the permission screen.

Consider an app that not only requires permissions within the "Other" group but now also requires permission to access location. Albeit this group will now appear on the permission screen, the new group(s) are not highlighted so the user can easily miss the new addition.

In summary, users have to agree to groups of permissions, grant permissions as before, as a blank cheque, but also implicitly grant future unknown access permissions within the same group. These will be taken without consent, nor

will they even be brought to the user's attention. If they are, they will be hardly discernible. This opens the floodgates to potential misuse.

On top of this, the respective hint is printed in such a small font, if it appears at all, that users could easily miss the change. Thus, with each update, privacy might be increasingly violated, slowly and imperceptibly without the user's knowledge.

3.4 Unintuitive Permission Allocation to Permission Groups

In some cases apparently thematic matching permissions are inexplicably allocated to different groups. For example the permission group "Identity" contains the permissions "Get Accounts"[2] and "Manage Accounts"[3]. The permissions "Authenticate Accounts"[4] and "Use Credentials"[5], however, are found under "Other" and are not visible to the casual user during installation.

This practice could confuse the user. Without complete knowledge of the required permissions the user has to make assumptions about the permissions the respective app will require. Another example of this kind of practice can be found in the permission group "Device and app history". It contains the permissions "Read bookmarks for websites and the web protocol", whereas the permission "Write web bookmarks and history" is sorted into the group "Other". A similar incongruency is the presence of "View Wi-Fi connections" in the group "Wi-Fi connection information", but not the permission "Connect and disconnect from Wi-Fi" which can be found in the group "Other".

This means the user cannot trust the information given on the permission screen when installing an app. Because of this inexplicable allocation of permissions to groups, the user's privacy is endangered since they are likely to miss relevant changes concerning the access permissions of apps. Consequently they might inadvertently allow apps to access their private data.

3.5 Explanations for Unintegrated Permissions

Informed risk assessment and the subsequent privacy-related decision is made more difficult because explanations are unavailable on the Google Play Store itself. The user has to use external sources such as websites or third parties to obtain information. The other option is to install the app first and check the permissions in the system settings afterwards.

Deep in the system settings of Android one can gain access to a list of all installed apps and, with a touch, all details about the app are displayed. This is the only place users can find an explanation of each and every permission. The categories used here are, unfortunately, different from those used in the Google Play Store (at least for the most recent Android version 4.4.4). For example, with regard to the depiction in Figure 2(a) in the system setting of "Wetter App" the term "Photos" or "Media" cannot be found at all. Instead you find a USB Logo in the respective permissions list. The permissions of the group "Other" are split up into three other categories, that are marked with a key-symbol ("Read google service configuration"), a Wi-Fi-Symbol ("Full network access") and a battery-symbol ("Control vibration") respectively.

Installing the app and checking the permissions later is, of course, not an appropriate way to proceed if one wants to preserve privacy. The app receives all required access permissions at installation and belated checking and possible de-installation cannot reverse a privacy violation that has already occurred. Due to the missing explanation of the permissions it becomes complicated to make an informed decision about the required permissions of an app. To make an informed decision the meaning and implications must be clear.

3.6 Impersonal and Harmless-Sounding Permission Descriptions

The new permission descriptions seem more technical than the previous ones. For example, the old explanation said (access to) "Your Location" , "Your Accounts" or "Your personal data". In the new implementation this corresponds to the terms "Location" and "Contacts/ Calendar". A semantic reference to the individual person is clearly avoided so that a user tends to associate more with "function" than with "personal privacy". By renaming the permission groups a depersonalization is achieved so that inexperienced users who are less familiar with technology, a large number, will tend to underestimate the granted permissions, and not perceive them as applying to themselves and their personal data. This could exacerbate the tendency to ignore the permission screen completely and unintentionally gift personal data to third parties, thus inadvertently endangering privacy. In the same vein is the statement "needs access to" located at the top of the permission screen. This statement is likely to convince an inexperienced user to the idea that everything is needed to implement the required functionality. In reality it might be requested simply because the developer thinks it could be handy. Users might easily compromise their privacy due to having gained the wrong impression.

4. CONCLUSION AND OPPORTUNITIES FOR ACTION

With the new permission screen Google changed many things. Based on their own statement [6] in order to make it easier for the user to make an *informed decision* whether an app shall be installed or not. Abstraction of the complete list of all requested permissions into thirteen permission groups with symbols as recognizable intuitively as possible shall enable the user to understand more easily to what an app will have access based on its permissions. If users want all information about the requested permissions they can only reach these via "permission details" which are placed at the end of the

[2]Allows an application to get the list of accounts known by the phone

[3]Allows an application to perform operations like adding and removing accounts and deleting their password

[4]Allows an application to use the account authenticator capabilities of the AccountManager, including creating accounts and getting and setting their passwords

[5]Allows an application to request authentication tokens

[6]Based on the online documentation "Review app permissions" by Google; last conduction September 29^{th}, 2014

app-detail-page. The "normal" user who just presses "install" will not see a large number of the requested permissions and is probably not even aware of this! In Germany, where the authors of this article live, response in the general media was rather muted [7]. Exclusively technology-specialized media such as heise online [11], golem.de [8] or areamobile [3] as well as androidnext [2] dealt with this topic. These sources comment mainly on the fact the user now has to grant authorization to permission groups and no longer grants single permissions, which can lead to a serious escalation of access rights to apps without the user's knowledge in case of activated automatic update (as described above). High-coverage German speaking general online media such as www.faz.net, www.spiegel.de or www.bild.de did not even report. A similar search for English speaking sources (search words: "permission screen play store") draws the same picture. So far only technology-specific media has published reports about the changes. For example www.xda-developers.com wrote about the possibility of significantly extending access rights via the auto-update function. They referred to a thread on www.reddit.com where a user coded an example app which requests many more permissions after an update to confirm this possibility. We could not find any articles in general English speaking online media with high coverage (e.g. www.wired.com or www.bbc.co.uk).

The user is left with this problem. There remains only the possibility of individually deactivating the auto-update function for each app and checking each update manually via the "permission details" link at the end of the app-detail-page.

The new permission screen is limited to showing only the names of the groups. This may result in the situation where an app that requests four permissions within one group seems to have fewer permissions than one that requests one in each of two different groups. Keeping in mind users mostly do not understand the complex permission structure of Android [12] and the fact that people tend to simplify complex decisions via heuristics makes this abstraction alarming. For example, someone could have a heuristic that says: "fewer permissions are better". This could lead them to misinterpret the true extent of the permissions they are granting.

The new implementation does not make it possible for users to make *informed decisions* (Google's term). If users, for example, want to install a QR-Code-Scanning-App that only requires (justified) access to the camera functionality [5] they will probably be confused as this request is expressed unclear ("Uses at least one of the following elements: camera(s), microphone(s)") thanks to the new abstraction. Wary users have no choice but to go via the complicated route of accessing "permission details" at the very bottom of the app-detail-page for each potentially interesting app. Even if we assume the ideal case of a user who carefully reads online resources about the new Google implementation there is still a risk because of the initially invisible group "Other".

Although Google explicitly says that the user will *always* be asked to check changes, those changes only appear in the difficult to find "permission details" at the bottom of the app-detail-page. Most users probably don't even scroll down to look at these. Even changes in the twelve shown groups are not highlighted so checking these is challenging. Users might even believe that the store operator tests all apps and deletes dangerous ones [10].

In this respect it seems plausible that in reality the most likely situation seems to be one in which users have not read the documentation and therefore only know the screen following the "install" irrespective the "update" button. They are not aware of any problems, because they do not even know the permission group "Other" exists. Users cannot be expected to initiate searching for another screen or assuming that they have not seen all requested permissions. At this point it is up to Google itself, as well as to the research community, to clarify and develop better solutions.

Within the research community a number of different proposals to improve the depiction of the requested permissions [inter alia [10, 13, 14, 15]] have appeared. They wish to empower the user so as to harmonize his individual wishes concerning his privacy with selection of apps to be installed. An extensive analysis and a comparison of the effectiveness of the different approaches is still missing.

Among other things the research project ZertApps[8] supported by the Federal Ministry of Education and Research in Germany comes in at this point. Within this project researchers from Bremen and Darmstadt collaborate to integrate solutions which provide tools for the user in order to preserve his privacy. While doing this it is essential to investigate the comparison of already proposed solutions and the importance of information that is not easily derived from the requested permissions. For the user it could be of major relevance to know with which partners an app is exchanging data with. This will help him to decide whether he has enough trust in the app and its interaction partners to permit access to his personal data. Furthermore, for the assessment of the application context it could be very important to see why an app requests a certain permission, i.e. which function it supports.

The benefit of such information in supporting privacy-related user decisions must be assessed. Moreover, possibilities to integrate these in a understandable and usable way into the graphical interface must be developed. In such a way usability and privacy could potentially no longer be antagonists but integrated concepts.

5. ACKNOWLEDGEMENTS

This article was supported by the German Federal Ministry of Education and Research in the framework of the project "ZertApps".

6. REFERENCES

[1] Android.com. Manifest.permission. Retrieved December 15th, 2014. http://developer.android.com/reference/android/Manifest.permission.html.

[7] A Google search with the terms "Berechtigungsanzeige Play Store" for the period from May 1*st*, 2014 till July 31*st*,, 2014 resulted in only five German hits. (last conducting October 1*st*, 2014)

[8] http://www.zertapps.de/

[2] androidnext. Google Play Store: Jüngstes Update sorgt für laxere Handhabung von App-Berechtigungen. Retrieved December 1st, 2014. http://www.androidnext.de/news/google-play-store-juengstes-update-sorgt-fuer-laxere-handhabung-von-app-berechtigungen/.

[3] areamobile. Google erschwert Prüfen von App-Berechtigungen. Retrieved October 1st, 2014. http://www.areamobile.de/news/27347-android-google-erschwert-pruefen-von-app-berechtigungen.

[4] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is everything? In *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, page 319, New York, New York, USA, 2009. ACM Press.

[5] Fachbereich Informatik Technische Universität Darmstadt. Forschungsgruppe Security, Usability and Society: Privacy friendly QR Scanner App. Retrieved December 15th, 2014. https://www.secuso.informatik.tu-darmstadt.de/de/research/results/privacy-friendly-qr-scanner-app/.

[6] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. Android permissions demystified. *Proceedings of the 18th ACM conference on Computer and communications security - CCS '11*, page 627, 2011.

[7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner. Android Permissions : User Attention , Comprehension , and Behavior. In *Symposium on Usable Privacy and Security (SOUPS) 2012*, Washington, DC, USA, 2012.

[8] golem.de. Android-Apps erhalten leichter mehr Berechtigungen. Retrieved October 1st, 2014. http://www.golem.de/news/google-play-store-android-apps-erhalten-leichter-mehr-berechtigungen-1406-106856.html.

[9] Google. Check app permissions. Retrieved September 29th, 2014. https://support.google.com/googleplay/answer/6014972?hl=dehttps://support.google.com/googleplay/answer/6014972?hl=de.

[10] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. *Proceedings of the 32nd annual ACM conference on Human factors in computing systems - CHI '14*, pages 2647–2656, 2014.

[11] heise online. Play Store ermöglicht Apps mehr Rechte ohne Nachfragen. Retrieved October 1st, 2014. http://heise.de/-2211827. retrieval date: May 30, 2014.

[12] P. G. Kelley, S. Consolvo, L. F. Cranor, J. Jung, N. Sadeh, and D. Wetherall. A Conundrum of Permissions: Installing Applications on an Android Smartphone. In J. Blyth, S. Dietrich, and L. J. Camp, editors, *Financial Cryptography and Data Security*, volume 7398 of *Lecture Notes in Computer Science*, pages 68–79. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[13] P. G. Kelley, L. F. Cranor, and N. Sadeh. Privacy as part of the app decision-making process. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, page 3393, 2013.

[14] L. Kraus, I. Wechsung, and S. Möller. Using Statistical Information to Communicate Android Permission Risks to Users. In G. Lenzini and G. Bella, editors, *Proc. of 4th Int. Worshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE, 2014.

[15] H. S. L. Z. Lin, Amini. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing. pages 501–510, 2012.

[16] T. Vidas, N. Christin, and L. F. Cranor. Curbing Android Permission Creep. In *W2SP*, 2011.