Encouraging Privacy-Aware Smartphone App Installation: What Would the Technically-Adept Do?

Oksana Kulyk*, Paul Gerber*, Michael El Hanafi*, Benjamin Reinheimer*
Karen Renaud†, Melanie Volkamer*‡
*Technische Universität Darmstadt, Germany
Email: name.surname@secuso.org
†University of Glasgow, UK
Email: karen.renaud@glasgow.ac.uk
‡Karlstad University, Sweden

***Abstract*—Smartphone apps can harvest very personal details from the phone with ease. This is a particular privacy concern. Unthinking installation of untrustworthy apps constitutes risky behaviour. This could be due to poor awareness or a lack of know-how: knowledge of how to go about protecting privacy. It seems that Smartphone owners proceed with installation, ignoring any misgivings they might have, and thereby irretrievably sacrifice their privacy. In this paper, we focus on the lack of know-how. Our primary aim was to design a set of guidelines to help Smartphone owners to judge whether apps are likely to respect their privacy or not. To produce these we investigated the stances of those who *do*, to some extent, have the requisite awareness and knowledge, namely those with experience in IT security or computer science in general. Such technically-adept people can reasonably be expected to apply pattern-like heuristics when making installation decisions. We carried out a study to identify and describe their heuristics. We then distilled their app-related decision processes into a set of easily accessible guidelines and we conclude the paper by providing these.**

I. Introduction

Smartphones are gaining prominence in many people's lives. As a consequence of their ubiquity and usefulness, they accumulate large amounts of data, much of it sensitive and personal.

The most commonly used Smartphone operating systems, iOS and Android, implement mechanisms to ensure people are informed of all data apps will gain access to. The Android OS offers a list of app permissions during installation. iOS apps request access to data during runtime, so that iPhone owners have more fine-grained control than pre-Android 6.0 versions. Furthermore, app developers are encouraged to present privacy policies to the Smartphone owners that enumerate the types of data being collected by the app, and to explain how this data is stored and processed[1].

[1]https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_10_mobile_controls_and_design_principles, Section 7. Accessed 18.12.2015

USEC '16, 21 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/usec.2016.23016

Many Smartphone owners grant data access to apps that effectively commit widespread privacy invasion [7]. For some of them, the reason might be lack of awareness regarding privacy issues, so that they do not even see the need to protect their privacy. Another group of users, however, might well be motivated to protect themselves – and yet fail to do this due to a lack of pertinent know-how.

People who extensively study, research or work in computer science, on the other hand, *can* be expected to have the requisite know-how. Although they might not necessarily have the expertise to consider the social implications of privacy, they can still protect themselves by applying their technical knowledge to their own private Smartphone usage. We report here how we went about uncovering the judgement heuristics of the technically-adept. We wanted to elucidate the implicit processes they applied when choosing to install Smartphone apps, or not.

We distilled these into a simple and manageable set of signposts which could be used to inform users' app installation decisions. Adopting even a subset of the listed heuristics can be helpful. In addition to supporting Smartphone users, the guidelines could also be helpful to certifiers or developers of corporate policies, specifically those whose task it is to approve Smartphone apps for corporate use.

II. Study Methodology

Here we describe the interview design and how we analysed the interviews.

A. Study Design

We conducted semi-structured interviews, the shortest of which took 43 minutes, and the longest 78 minutes. The interview was structured as follows:

a) Warm-up: First we asked the participants about their experience and their current work. This was done in order to estimate their level of technical knowledge and familiarity with Smartphone privacy aspects. This question allowed us to filter out those who lacked the requisite knowledge to contribute to our heuristics collection. The remaining participants demonstrated an understanding of privacy concepts and of the measures that ought to be taken in order to protect privacy.

b) Demographics: We asked about the type of Smartphone they owned, and their usage thereof. We also asked them how many apps they had on their Smartphones, and how often, and on which occasions, they had installed them. We asked about whether they had rooted or jailbroken their phones, and their reasons for so doing, or refraining from so doing.

c) App installation: The main part of our interview required participants to perform a task on their Smartphone. They were asked twice to choose an app that they *would* install on their Smartphone, and to comment on their thoughts during the installation process. The participants were not required to actually install the app; their task was merely to select the app they would consider installing. We chose two types of apps for this part. In the first task the participants were asked to choose a Sudoku app, since such apps would normally require few to no permissions. In the second task they were asked to install a photo-editing app capable of some basic functionality. We chose this type of app because apps of this type tend to be rather complex and require a large number of permissions. Some of these are mandatory in supporting their basic functionality, others perhaps not. This would help us to gain insight into how our participants behaved since the two kinds of apps varied in terms of complexity and data privacy aspects. After completion of the tasks, the interviewer asked the participant to clarify the motivations for their choices.

d) Recommendations: The participants were asked to give general recommendations related to app installation that they would give to those without technical knowledge.

B. Recruitment

For the purposes of this study, we recruited participants with experience in computer science, either in industry or in academic research. While we focused on people with knowledge in IT security, we also considered people from non-security related computer science research areas, due to their having more technical knowledge than the general population. The participants were recruited via the snowball principle, using emails sent to the departmental colleagues of the authors. They were offered no reimbursement for their participation.

C. Participants

The study had 26 participants, all of whom were computer scientists. Of these, 19 were working specifically in the field of IT security, from theoretical cryptography to Android security. The rest were from other computer science research areas, such as computer linguistics and graphics. There were five graduate or undergraduate students, 13 PhD students, five PhD graduates working at the university, one PhD graduate working in industry and two professors. The gender ratio was six female and 20 male participants. Seventeen participants owned Androids, eight owned iPhones, and one owned a Windows Phone.

D. Analysis

The interviews were transcribed and analysed using an open-coding approach. The goal was to identify privacy-related heuristics that the participants either used themselves for app search and installation, or recommended to others. For this, specifically interview parts II-A0c and II-A0d were considered, although in some cases some relevant heuristic was mentioned by the participant earlier during the interview.

Each interview transcript was read by at least two authors. Each composed a list of categories and subcategories of the heuristics to classify the findings, which were then discussed and agreed upon in the group. The (sub)categories were then supplemented with the quotes from the interviews, translated from German into English. Since our goal was to perform a qualitative, instead of quantitative, analysis we did not count the number of times each suggestion appeared in interviews. We also did not include the heuristics that were clearly based on concerns other than privacy, such as for example the color-set of the interface.

III. Results

We derived following categories of heuristics from our analysis.

e) Permission-related: The heuristics in this category rely on using the list of permissions that the app requests as a basis for a decision. This category has following sub-categories: *judging whether permissions are reasonable* and *judging whether permissions are acceptable*.

f) Developer-related: The heuristics in the next categories focused on the developers, gauging their public image, development process and the quality of related products. The sub-categories are: *judge the developers themselves*, *judge app currency* and *judge based on related apps and services*.

g) Socially-related: In this category, the heuristics are based on social factors related to the app. The following subcategories were derived: *other people downloaded the app*, *other people recommended the app*, *other people's reviews* and *other people's ratings*.

h) Avoidance techniques: The final category included the heuristics that specifically focused on minimizing either sensitive data exposure to the apps, or app usage altogether. The subcategories are *avoid apps*, *avoid data leakage* and *avoid negative vibes*.

We further identified some conflicting heuristics, whereby the participants' opinions differed on what action would be more optimal for privacy or security assurance. Such discrepancies could be grouped into following categories: *rooting*, *Apple vs. Google* and *using cloud services*.

We elaborate on each one of these findings in sections that follow.

IV. Permission-Related Heuristics

App permissions were a strong theme. The types of data access required by the app was considered an important factor for deciding whether to install it.

A. Judging whether Permissions are Reasonable

The most commonly mentioned heuristic supporting the installation decision was whether the permissions that the app requested made sense given the app's purpose and functionality. For this reason, many participants decided against installing an

app, both Sudoku and photo editing, that required permissions whose purpose did not match the app's functionality.

Several heuristics have been proposed for deciding whether some permission is appropriate for the app, or not. The most straightforward of these was to identify permissions that are necessary for the main functionality of the app. For the photo editing app this was the permission to access stored photos.

> *"A photo editing app needs access to my photos to be able to work."*

Other participants also examined the app description to detect additional features which might warrant requesting a particular extra permission. They could identify these features either by reading the app description provided by the developer, or they could try to figure it out themselves by considering which features would be expected from this type of apps.

> *"I would look at the app description, to find a reason for those exceptional permissions. I mean, it could be possible that there is a special function like being able to recommend this app to friends and therefore you would need to send emails to contacts from your address book. If I could understand the process, so that this wouldn't be an automatic process, but an extra feature, it would be ok."*

It was seen as an advantage if additional permissions, the purpose of which was not self-evident, were explicitly motivated in the app description. The app description was perceived to be an opportunity for developers to provide explanations for permission requests and was therefore examined carefully if a permission request looked unnecessary.

> *"A Sudoku app normally doesn't need my location nor access to the Internet. Unless it provides a significant added value. But, this must be explained in the app description by the developer, since the core functionality of a Sudoku-app isn't to download something from the net."*

B. Judging whether Permissions are Acceptable

1) Acceptable: In some cases, the participants were willing to grant some permissions independent of the app functionality. As such, the risk for allowing a concerning permission was accepted if the permission could be blocked by means of special external tools, such as those provided by CyanogenMod[2], an alternative operating system.

> *"I do not generally have problems with this, because I have also installed something that I can use to block all the stuff. Namely, even if the app wants a relatively high number of permissions, I simply block the ones that I believe should not be granted."*

Participants mentioned other ways of preventing apps from utilising granted permissions, such as turning off WiFi while using an app, or closing the app running in the background when it is no longer needed.

> *"It is concerning that one can find out where I am, but as far as I know it is only possible when the app is on, and I kill apps that I no longer need"*

> *"Then I uninstall it immediately. If I need it only for this specific one time use, then it is not so simple to get information, because I just turn off mobile data and WiFi, then it cannot transmit data."*

Another reason for generally accepting some of the permissions was that the participants were not concerned with the risks that particular permissions represented, due to either not storing sensitive data that an app might access on their phones, or generally finding it acceptable to reveal such data.

> *"I find In-App purchases non-critical, because I have no credit card information there."*

In particular, one of the reasons not to be concerned was that the shared information was likely to be deducible from publicly available information anyway.

> *"...it would be much less pleasant than if it only knew my location and where I was. Since one can also find out in many other ways, that, for example, I work in [anonymised]. Then it does not signify that [the app] knows my location, or not."*

2) Unacceptable: Some participants mentioned that they had never given particular permissions, or only rarely, in very extreme circumstances. The kinds of permissions that fell into this category were location data, details about phone calls, contacts, and, in general, personal data about one's family.

> *"For example, the photos of my family, access to some E-Mail accounts or something. This is sensitive data. Or some bank transactions. [...] Location also belongs to very sensitive data. And whatever ID means. [...] I try not to give any access there, as much as is possible."*

V. Developer-Related Heuristics

The following quote shows that if one accepts permissions that are essential to support the app's main functionality there is still the need to trust the developer's integrity i.e that he is not misusing the granted permissions for other purposes:

> *"...at the end of the day every permission is a certain risk — do I accept the risk or do I have enough trust that this permission is not going to be abused?"*

Our participants judged the app developer using a number of criteria. Most mentioned gaining a holistic impression of seriousness or reliability of the developer, as derived from different factors. While some of the factors are assessed objectively, deriving the overall judgement is a complex task and even the technically-adept sometimes have to rely on their intuition.

> *"If my gut feeling tells me the developer is ok, I would maybe do this, but with a bad gut feeling I would definitely drop it."*

The enumerated factors and criteria are described in the following subsections.

[2]http://www.cyanogenmod.org. Accessed 18.12.2015

A. Judge the Developers Themselves

1) Existing Reputation and Publicity: The most frequently cited criteria was the developer's reputation especially that of the company. Being able to see the name of the developer, especially if it was a big company or a long established brand, was a positive aspect for most of our participants.

> *"I would recommend downloading apps developed by well-known developers instead of run-of-the-mill-developers, since well established developers probably have quality management under control and are likely to fix bugs. Additionally the probability their products contain malware is smaller."*

The participants mentioned different reasons why they see positive aspects in this. First of all they assume that a big company cannot afford to knowingly deliver malware and it is less likely that they would risk their well-established brand name by promoting an app that invades customer privacy since a good reputation is a valuable yet fragile asset.

> *"... well-known companies can't afford to knowingly provide malware in their apps. This would ruin their business."*

This is also connected with good experiences in the past and on other platforms such as the PC. Brands that are known for their reliability on other platforms are perceived to be more likely to perform well on Smartphones.

> *"Yes, since Adobe is kind of an embodiment of photo editing. It is a well established brand."*

Although a known name is a positive sign some of our participants also mentioned that just knowing the brand, on its own, is insufficient. They mentioned that they searched for more details even if they knew the developer or his/her company. This applied especially to apps with extensive permission requests since in this case trust in the reliability of the developer was crucial.

> *"So ... if I just heard the name once, I examine them more closely. Initially I didn't trust any developer ... trust will build up while checking him. This, of course, didn't result in not installing apps from unknown developers at all. This app with the cow, this to-do app, I have no clue who developed it but it didn't request extensive permissions so this was ok."*

Also often mentioned as being important was that nationality of the developer. Some participants specifically mentioned trusting German developers more since the German Data Protection Act is more restrictive and overall privacy is given more consideration in Germany than in other countries.

> *"I would normally take a closer look at the developer of the software. Especially if it is sensitive data ... hm ... Here I maybe would say, a German developer is more trustworthy to me than a foreign one, since privacy plays a really important role in Germany as compared to other countries."*

Participants also mentioned concerns about developers using servers in countries with opaque Privacy Acts such as China or Russia.

> *"Whether the developer's name seems trustworthy to me ... hm ... this depends on which data it requests. Also which servers are contacted in the background. I'm no friend of apps that communicate with some Russian servers. Maybe a bit uninspired ... or some Chinese servers, no offence, but I would prefer my data remain on German servers or American or so."*

Last, but not least, the impact of past events, especially a privacy or security related event, made participants reconsider the reliability of a developer. This goes for the app in question but also the associated brand or company.

> *"Maybe one can recall another piece of software about which one has heard something negative. Maybe it had some security holes or something like that. If the same company produces this app I could assume maybe there also is such a risk."*

> *"I would guess it would be in the news, because such things, like big apps publishing your data without telling you, always makes a good story. Therefore I would expect that if something comes to light, I think we had this with WhatsApp a couple of times, then I would sooner or later read about it in the newspaper."*

2) Developer's Webpage Content: Checking the developer's web page was considered a crucial part of the assessment process. The layout and content of a developer's page provides, analogous to the app description, objective information such as manuals, tutorials and privacy terms as well as subjective information about the quality of service provided by the application. Some of our participants mentioned that they associate a poor quality web page with a likelihood of a lower quality app.

> *"You also get a certain feeling whether quality is a concern to this developer or not if you check the layout of the web page. Since this is the public representation of the company ... if this is carelessly designed I would assume they are working carelessly and therefore their software is also produced without care."*

For some participants, one of the important parts of the web page was the presence of privacy-related terms. The mere existence of documentation about data usage was considered essential. Even if no data was collected and transmitted by an app, such a document ought to exist.

> *"If they didn't write anything about data privacy, I would drop it. If they wrote something awkward there, I would drop it. Even if they don't collect anything they could afford to write a single sentence 'We do not collect any data.' and that's it, matter straightened out. If they don't do it I'm better off."*

Sometimes seeing privacy terms was not considered sufficient. In these cases the content was carefully perused. They searched for data leakage which is not considered necessary for providing the service itself and therefore goes beyond their own expectations.

"I would search for something awkward, in particular for data usage over and above the expected. Namely, if they write that they store my mail address and all data you send while contacting us it is ok. Or, if they store my pictures while I use their cloud services. These are things which are necessary in order to provide the service itself. Besides I can't determine how the stored data is processed from a technical point of view. If I want to use their services, the ease of the cloud, I have to provide my data, this is no problem. But if they collect data which is not directly linked to the service itself, this should be a warning. This activates a red flashing in my head."

Moreover participants also considered additional features on the web page to be a positive sign. These include bulletin boards, newsgroups or the opportunity to get in touch with the developers to request new features or give feedback to already-implemented ones. This applies especially to more complex apps.

"If it is Software which is difficult to use or has a long feature list, I would search for manuals or something like this. It is also useful if there is a bulletin board where users can ask questions or a newsgroup. Or the possibility to contact the developers, maybe to request new features or so."

As a motivation for installing an app, some participants also mentioned not only their own goals and privacy concerns, but also their willingness to encourage some particular developer behaviour.

"In principle, one can also make a Sudoku app completely without permissions. This is, of course, a bad business model, so, when someone is so nice, then it is good, I would gladly support this by installing this app."

B. Judge App Currency

In the assessment of developer reliability questions about maintenance were considered by our participants. Since software can potentially have bugs and security holes, a regular patching and updating philosophy seemed crucial. Therefore participants checked the recency of the last update.

"... this was last updated on the 20th of January 2015. This one, on the contrary, was last updated on the 10th of February 2013, so it is significantly older and obviously no longer maintained. Maybe this would be the criteria."

C. Judge Based on Related Apps and Services

Last, but not least, an assessment of other products by the same developer was mentioned. This goes especially for unknown developers. Participants check whether other apps in the marketplace exist and have good ratings and reviews or other users complain about their products.

"There you can check the ratings and reviews ... hm ... and how much apps they published."

"... if it is from an unknown developer, I check the Internet whether I can find something about it or if other users complain about their products"

VI. Socially-Related Heuristics

Common methods for estimating the app trustworthiness involved looking at social feedback: unfamiliar usage, peer-usage, reviews, ratings, experts or media reports. Almost all participants mentioned at least one of the six so we can conslude that they account for a large proportion of the deployed heuristics.

A. Other People Downloaded the App

A heuristic shared by a large number of the participants was the number of downloads. The more downloads an app has, the more trustworthy the participants considered it to be. The rationale behind this assumption was the "self-cleaning process" of the appstore. Untrustworthy apps would be removed before it could amass a large number of downloads. The large number of downloads suggest that there is "no problem".

"Regarding the apps, that are popular and downloaded a lot, yes, I would trust that there would be some people who would notice any [privacy issues]"

B. Other People Recommend the App

Participants often asked friends for advice, especially when they had specific functionality in mind. Soliciting recommendations when the participants consider their own knowledge to be insufficient seems a popular heuristic.

"So, for me it would be nice to have a recommendation from a competent friend, or it does not have to be a friend, just a competent person, where I think that he watches out for the kinds of things I would watch out for."

C. Other People's Reviews

Reviews from other app users tend to inform many participants. In particular, some specifically searched for mention of privacy-related issues.

"But if there is something like, for example, real malware, where someone had noticed, while having a firewall on his phone, that the app tries to send data to some server that has nothing to do with what the app does, this would be, for me, a criterion to reconsider whether to install such an app."

Alternatively, when the participants themselves were not sure whether the requested permissions were reasonable, they scanned the reviews to gauge the opinions of others.

"For example, when the app wants to access different things, if reviewers say this makes no sense [...] then I do not like this at all. [...] Since I am sometimes not so sure myself, in terms of what makes sense and what does not, and when many people write that it makes no sense to access this, then it is something negative for me."

Keeping an eye out for "bad reviews" seemed to be a helpful strategy for some of the participants. They mentioned focusing on these to detect a worst-case scenario. If this worst-case scenario did not contain anything "terrible", they would go ahead and install the app.

> *"Well I find it interesting to know when people give really bad reviews, whether they are based on something fundamental or not."*

Some participants consulted usability reviewers' reports to inform their decisions.

> *"What could be of interest too are the number of advertisements displayed, just from of usability perspective, well advertisements are the one thing that mostly ruins usability."*

Numerous participants considered forums and other online communities to be a valuable source of information.

> *"One should take [the app], because the crypto community says it is good. [...] So that, at the end of the day, one knows what is the right one, and one has to dig through a bunch of forums and articles and blogs..."*

Others mentioned specific websites they visited while looking for an app. On the one hand writers on such websites are expected to have a deeper and broader knowledge. On the other hand, time-consuming comparisons between different apps are outsourced to such websites because of their presumed knowledge and the person's own lack of time to do this themselves.

> *"In general I would simply search online for apps. Looking for some bulletin boards or maybe you find something on well-known pages such as CHIP which lists such apps. These are trustworthy."*

D. Other People's Ratings

App ratings e.g. the number of stars in the Android Appstore, was relied on by some participants.

> *"I would expect that some kind of crowd intelligence would also become apparent in the ratings, if some app is not recommended. Also when most of the users do not seem to care about security."*

E. Contact Developer

Finally, if all these sources did not prove sufficient to support a decision some participants would contact the app developers directly.

> *"I would ask the developer [...] but most likely I would try to get in contact."*

VII. Avoidance Techniques

Some of the heuristics focused specifically on avoidance, where participants chose either to minimize usage of apps (either overall, or of apps of certain kind), prevent wholesale leakage of data, and generally avoiding negative intuitive feelings they might get from apps. The following were mentioned:

A. Avoid Apps

1) Minimise App Installation: Most apps require some permissions, potentially accessing sensitive data. This could be misused. Some participants recommended minimising these risks by having only essential apps on their phones.

> *"I only install apps when I really have a very concrete feeling, that it would help me [...] just consider if I really need this app."*

To keep track of all apps, some recommended filtering out those that are no longer in use.

> *"It would also be good to delete unnecessary apps from time to time"*

2) Look for Privacy-Sensitive Alternatives: Since evaluating the validity of requested permissions can requires effort, some suggested minimising this effort by choosing apps that are less complex, have less functionality, and thus request access to less data.

> *"Now with these big apps with 21 features, in this situation one cannot decide, whether the permissions are really alright or not. Then, I mean, in most cases it is possible, that there is an app, that can do only 3 things, and one of them is what I want to do. These are simpler to check. "*

> *"Therefore the recommendation would be, when you are unsure, try to find a simpler App that is not such a huge thing, but does what you want. "*

3) Avoid Free Apps: Although many participants admitted never, or seldom, paying for apps and preferring free alternatives, several acknowledged that free apps might collect more data than those that one paid for. Some were willing to pay for apps in exchange for the privacy they thought this would give them.

> *"I would, in any case, rather buy an app, in order to free myself from the permissions, than accept too many permissions."*

B. Avoid Data Leakage

Some participants suggested storing their personal and sensitive data somewhere less vulnerable, such as on their PC.

> *"or even better, do not store photos there, or, if possible, transfer them. [...] then I can store them on my PC so that they are there but i still can use the [app].*

As a radical solution, some participants proposed using a second device for this purpose, one that did not contain any sensitive data on it. This suggestion, albeit not practical for many, was indeed a viable solution, particularly for those participants who worked on Smartphone security and therefore had a variety of test devices available to them.

> *"Or, get yourself a second Smartphone and install everything on it, since it would not make any difference"*

C. Avoid Negative Vibes

Some participants admitted relying mainly on their intuition, formed by their technically-rich experiences, informing their security-related decisions.

> *"This is a feeling I get as a computer scientist."*

Such an approach is used for various tasks, such as evaluating the appropriateness of permissions requested by the app, or the trustworthiness of the developer while assessing the privacy terms.

> *"Yes, the privacy policies are mostly so confusing, I do not normally read them through. So, it is mostly an intuitive decision."*

> *"For me, it would be my intuition. And I mean, I have also programmed a lot of Android apps, and grappled with these permissions, therefore I know what is needed for what."*

VIII. Disagreements

Participants mostly agreed, or at least did not contradict each other, but some differing opinions were voiced. These are discussed in this section.

1) Rooting: A number of participants had rooted or jailbroken their Smartphones. Several also claimed that it helped them to protect their privacy. For example, they could install a firewall or permissions-blocking software that would not be possible on non-rooted devices:

> *"With it I actually wanted to install a firewall, for example, and for the apps that restrict the execution of other apps one needs root access."*

Others, however, held the opinion, that rooting delivered no significant advantages, and could actually harm the device's security by opening up vulnerabilities.

> *"I do not want to introduce security loopholes. [...] And when I say that an app has the possibility of getting root access, then it is already a lower level of security than to say, I have an operating system, that gives no one root access."*

2) Apple vs. Google: Not surprisingly, the iPhone and Android users differed in their opinions, in terms of whether Apple or Google was less or more likely to infringe their privacy. An argument for better privacy of Android was its openness and transparency, at least relative to Apple products.

> *"...then there was Apple, but they have such a restrictive policy, we decide what you do with your phone... I did not like it very much, and the Android phones were then very open."*

On the other hand, it was mentioned that Apple, as opposed to Google, gets its main revenue from sources other than data collection, and therefore is likely to collect and share less data than Google.

> *"Apple earns its money not with address data and similar stuff[...] I would assume, Apple does not share the data that they have with other companies. "*

3) Using Cloud-Services: Some participants were concerned about using cloud-services, perhaps for sharing pictures or organizing and syncing a calendar because of privacy concerns. One way to avoid this is to host your own server with cloud-services to maintain control over all the data.

> *"The point is, some of my data I wouldn't transfer to the outside world, but this depends on the data type. Some data is destined for public, so these can be stored anywhere but other things definitely not. [...] I have different apps which communicate with my own infrastructure at home. Such things like OwnCloud. Data isn't destined for foreign infrastructures, just for things like OwnCloud."*

> *"... if this app states: 'Hey I will store nothing locally but everything in the cloud.' This is really annoying. Such things must be decided by me alone."*

Some participants trusted well-established companies such as Google or Amazon since there would be a dedicated team responsible for security. This would minimise risks such as hacking and hardware malfunctions:

> *"Too much work. I mean, it is part of the functionality, that there is someone who maintains the system. Someone who works on such things such as backups and such things, all those annoying things I would have to deal with otherwise. And for this my data is an acceptable price."*

IX. Further Findings

A. Misconceptions

Even people with an advanced degree, or many years of experience, are not immune to misconceptions. This can easily occur via updates of the operating system or components thereof where unnoticed changes occur. For example the changes made by Google to the permission visualisation and grouping with Play Store Version 4.8.19 [8] which among other things removed the listing for Internet access from the pop-up permission list.

> *"I have looked for an app without access to the Internet, since Sudoku doesn't need such access and if it has, then the developer has to motivate this very well. Maybe to load new Sudokus, but even this isn't required since Sudokus could be generated offline."*

Another reason for such misconceptions could be transfer effects from other platforms as some participants assume that WindowsPhone 8.1 would display a pop-up if an app requests access to some sensitive resources such as the microphone or the camera. In fact each platform uses their own approach.

> *"I think he [the operating system] will ask me before installing whether I want to confirm such permissions or not, but this app doesn't request any. I mean access to the camera or my contacts or something like this. Such permissions will be requested, but this app doesn't need them."*

We also found a misconception regarding app testing. Some participants assume that trialing the app only costs them time

but in reality the app, while being trialled, accesses all the data and data leakage is possible even if it is un-installed after a few minutes.

> *"Hm ... yes .. first I would test the free one. It just cost me a couple of minutes to download."*

> *"Probably I just have to install and test them. Would have cost me just a little time."*

Some participants considered the risk of virus and malware to be low since Smartphones are not as ubiquitous as, for example, Windows PCs. This led them to believe that hackers would not produce viruses for these platforms. In 2014 around one point two billion Smartphone devices were sold worldwide[3], which is about four times the number of PCs sold in the same time period[4]. So this belief is misguided.

> *"In the past nearly everyone used a Windows PC, so it was profitable [to program a virus], but for MAC there were no viruses because of that for a long time. And now with Smartphones [...] the risk is relatively low because of the different operating systems on the market."*

Such examples illustrate that no one knows everything or unfailingly makes perfect decisions, not even those who consider themselves expers in computing. General expert knowledge of a domain, for example in our study general IT and security knowledge, can even be a handicap if it leads to over-confidence. Since the technically-adept probably know how to recover from adverse events they are sometimes equally likely to throw caution to the wind [16]. Acknowledging the human propensity for misattribution, suggestibility and bias is crucial.

B. Social Pressure

As social pressure sometimes plays a role in the decision process for laymen [17], even the technically-adept are not immune. Our participants cited pressure from friends or peers as a motivation for installing an app without checking for privacy issues or installing despite privacy reservations. In the following quote, the participant mentions installing WhatsApp messenger despite his concerns:

> *"...there was a colleague from abroad. He came to visit and said he wanted to communicate with me, and then I said: Fine, if it really needs to be.*

X. Deriving Guidelines

The following guidelines were and selected by three different factors, starting with only adding guidelines which were mentioned by at least one participants. Additionally we subjectively rated their practicability (e.g. a second device or special device isn't practicable for everyone) and effectiveness respectively plausibility (e.g. checking for interface colours is not useful guideline).

When participants were asked to give advice to privacy-unaware users, several of them focused on risk. The advice was generally to think about one's attitude toward privacy, and what consequences data sharing could lead to.

> *"One has to make up some rules, so that one can say: no, this is too much [data sharing for me]."*

> *"But [the user] should, in any case, extensively consider what relates to security. [...] he should in any case pay attention, that that data, that is being shared, would pose no problem to him."*

Several participants pointed to the importance of understanding exactly what the permissions mean, either by reading the descriptive text, or, if required, searching for further information via Google or by asking an expert.

> *"It would help to read, I mean, most [of the permissions] are explained correctly, it is written there, for example, can access these files, or, for example, read phone call status, and to whom the call was placed and something like that. So, just read and think about it using common sense, and, if needed, search the web."*

A. Guidelines

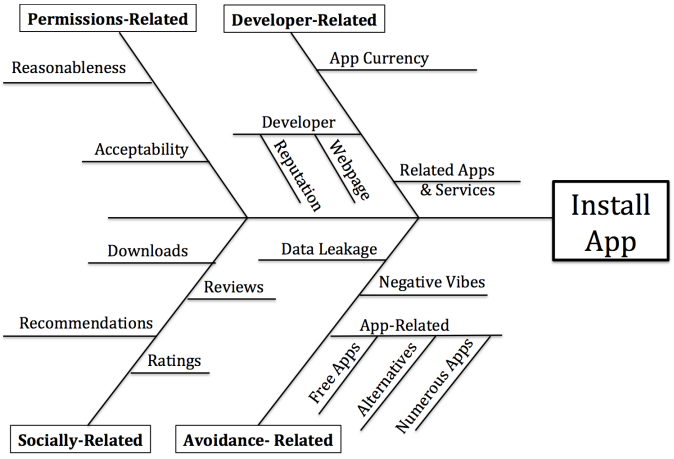

Fig. 1. Heuristics to Decide on Installation

Based upon our findings (Figure 1) and informed by the participants' recommendations, we were able to derive a list of guidelines for supporting users' privacy-related decisions concerning Smartphone apps. We first introduce the risk analysis concept, as this is what the users need to do before they can estimate the privacy of specific apps. Then we present a set of recommendations to inform their evaluation of the risk related to choosing and installing an app. Finally, we present guidelines on how to manage the apps already installed, in order to minimize unnecessary data exposure. Reference is made to the corresponding heuristic(s) for each recommendation.

Some of the identified heuristics are excluded from our recommendations, due to their being applicable only in specific use cases, mostly being applicable only to technically-trained Smartphone owners, those working in mobile development (VII-B, VII-C), or those expressing individual preferences (V-A2).

[3]http://www.gartner.com/newsroom/id/2996817. Accessed 18.12.2015
[4]http://www.gartner.com/newsroom/id/2960125, Accessed 18.12.2015

1) General Risk Analysis: As, ultimately, making a privacy-sensitive decision depends on subjective preferences, especially in private Smartphone usage, it is important for users to be able to conduct a rudimentary risk analysis. The steps could be summarised in following way:

1) Consider and take note of the **data** the app wants to collect. Note what exactly the individual app permissions mean. If it is not clear from the description, look for further sources of information. Trusted websites, your peers or experts are all good sources of advice. It is worth reading up so that your privacy-related knowledge is current. (X)
2) Think about the possible **consequences** if particular types of data are shared. Try to imagine potential scenarios if some information, such as photos stored on the device were to become public or fall into the hands of some malicious person. (X)
   Deciding which of these consequences are acceptable as a trade-off for the benefits the app provides. Depending on your **privacy stance**, you might choose to share as little data as possible, or you might be willing to trade privacy in exchange for desired functionality or reduced monetary costs to some extent. (IV-B2, VII-A3, VII-A1)

2) App-Specific Guidelines: The following methods could be used to estimate the risk presented by individual apps. The process outlined in Section X-A1 then serves as a basis to decide whether the risk is acceptable, or not.

Note that while many of these methods are general enough to be applicable to different mobile operating systems, some require different approaches. As such, while the Android user can always see the permissions required by the app *prior to installation*, this information might be more difficult to come by in iOS. Even though their might be changes in the operating systems e.g. new permission system in Android 6, most of the generic guidelines remain applicable. Checking the permission list beforehand still is important as runtime checking might lead to new mistakes e.g. miscalculating permission interaction.

B. Participants' Recommendations

These guidelines enumerate helpful preventative measures that will reduce the risk of app-related privacy violation.

1) Check whether the permissions are **suitable** to enable app functionality. In the best case, the only permissions requested by the app would be the ones that are necessary for its basic functionality. For example, one can expect a photo editing app to request access to photos. (IV-A)
   If the app offers extended features requiring additional permissions, one has to consider whether these permissions are still acceptable, or whether one should look for alternative apps requiring fewer permissions. If an app requires permissions that do not match the functionality this should raise alarms. (IV-A, VII-A2)
2) Seek out apps with larger user base: check the **number of downloads and ratings** in the app store. (VI-A, VI-D)
3) Look whether apps are being **actively developed**; check the last update date. This makes it more likely that the detected security vulnerabilities are corrected as they are revealed. (V-B)
4) Read **app reviews**, especially negative ones, to check whether they mention privacy issues, such as inappropriate permissions or some other kind of suspicious behaviour. It might also be helpful to check feedback outside of the app store by going to dedicated websites or forums, or consulting knowledgeable peers. (VI-C, VI-C, VI-B)
5) Research the **app developer**. You could check their website. The following factors might indicate that the developer is trustworthy:
   a) the developer is well-established, with several apps and large userbases, (V-C)
   b) the developer's residence is in a country that has privacy protection laws, (V-A1)
   c) the developer is a big company that values its reputation, (V-A1)
   d) the developer puts a privacy policy statement either on their website or in the app description. (V-A2)
6) Pay attention to **media reports** related to Smartphone privacy, since popular apps could be exposed if they violate privacy (V-A1).

1) App-Management Guidelines: Besides the recommendations to improve privacy awareness before installation, participants also provided recommendations related to the usage of installed apps.

1) If the app is installed, try to minimize **data sharing**. You could move sensitive data to a more secure storage venue, or ensure that the app does not continue to run in the background after it is no longer required. You could also turn off the Internet connection while using the app, so as to prevent it from harvesting your data. (IV-B, VII-B)
2) Regularly **review** all installed apps. Identify those that you no longer use, and remove them. (VII-A1)

XI. Related Work

A number of guidelines, either from government agencies or from private corporations, provide privacy advice to Smartphone owners [3], [4], [11]. These suggestions are either aimed at corporate Smartphone use or provide general information rather than giving specific step by step app installation advice.

Several studies have been carried out to investigate mobile privacy perceptions [15], [5], [14]. In particular, the studies carried out by [6], [7], [12], [2] focused on identifying mental models of the permission system in common mobile operating systems. The study in the last citation showed that, for laypeople, the impact of permission requests to support informed decision making appears rather inefficient. Even the addition of additional text warnings delivered no statistically significant

effect in terms of improving the impact of a permission warning. Other heuristics, such as an app's download count, seem more influential in terms of informing decision making. Some studies have investigated privacy perceptions in general [1], [13]. The reasons for users failing to deploy privacy-protecting mechanisms were identified using qualitative interviews in [17] with poor usability and lack of knowledge being considered major causatives. In [8] the changes made by Google to the Android permission visualization in the Play Store App were analyzed. Some major usability and understandability problems were identified.

An investigation into security expert attitudes and practices with respect to computer security was reported by [9]. The authors drew comparisons between the behaviour of experts and laypeople. They identified discrepancies between measures of privacy protection experts and non-experts deployed. A qualitative study, focusing on mental models of Internet security of experts as well as laymen, was conducted in [10]. This study found few differences between the behaviours of experts and non-experts. Given these conflicting findings it is clear that this topic merits more attention.

XII. Conclusions

Even if the users are motivated to protect their privacy on Smartphones, they might have difficulties making right decisions in their everyday usage without sufficient knowledge. Therefore, we set out to understand how technically-adept people reasoned about app installation so that we could derive guidelines to support these users.

We conducted interviews with technically-adept people with experience in computer science, the majority of whom were also working or doing research in in IT security, in order to identify their heuristics in terms of app installation. By performing a qualitative analysis of the interviews, we identified a number of deployed heuristics. We were then able to derive a set of guidelines for Smartphone owners.

Several discrepancies and misunderstandings emerged from our analysis and a further study should explore these in more depth. Future work will also determine the viability of these recommendations via user studies.

Acknowledgements

This paper has been developed within the project 'ZertApps', which is funded by the German Federal Ministry of Education and Research (BMBF) under grant no. 16KIS0073. The authors assume responsibility for the content.

This work has been co-funded by the DFG as part of project D.1 within the RTG 2050 'Privacy and Trust for Mobile Users'.

References

[1] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "Little brothers watching you: Raising awareness of data leaks on smartphones," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*. ACM, 2013, p. 12.

[2] K. Benton, L. J. Camp, and V. Garg, "Studying the effectiveness of android application permissions requests," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on*. IEEE, 2013, pp. 291–296.

[3] Bundesamt für Sicherheit in der Informationstechnik, "Überblickspapier Android," accessed 18.12.2015. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Android_pdf

[4] ——, "Überblickspapier Apple iOS," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Apple_iOS_pdf, accessed 18.12.2015.

[5] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 1.

[6] A. P. Felt, S. Egelman, and D. Wagner, "I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns," in *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2012, pp. 33–44.

[7] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: User attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, 2012, p. 3.

[8] P. Gerber, M. Volkamer, and K. Renaud, "Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy," *ACM SIGCAS Computers and Society*, vol. 45, no. 1, pp. 16–21, 2015.

[9] I. Ion, R. Reeder, and S. Consolvo, "... no one can hack my mind: Comparing expert and non-expert security practices," in *Symposium on Usable Privacy and Security (SOUPS)*, 2015, pp. 327–346.

[10] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler, "my data just goes everywhere: user mental models of the internet and implications for privacy and security," in *Proceedings of the Eleventh Symposium On Usable Privacy and Security*, 2015, pp. 39–52.

[11] Kaspersky Lab, "Smartphone security," accessed 18.12.2015. [Online]. Available: http://www.kaspersky.com/internet-security-center/internet-safety/smartphones

[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 *Financial Cryptography and Data Security*. Springer, 2012, pp. 68–79.

[13] L. Kraus, T. Fiebig, V. Miruchna, S. Möller, and A. Shabtai, "Analyzing end-users knowledge and feelings surrounding smartphone security and privacy."

[14] A. Lazou and G. Weir, "Perceived risk and sensitive data on mobile devices," in *Cyberforensics: Issue and Perspectives*. University of Strathclyde, 2011.

[15] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Understanding users' requirements for data protection in smartphones," in *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on*. IEEE, 2012, pp. 228–235.

[16] D. L. Schacter, *The seven sins of memory: How the mind forgets and remembers*. Houghton Mifflin Harcourt, 2002.

[17] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz, "A socio-technical investigation into smartphone security," in *Security and Trust Management*. Springer, 2015, pp. 265–273.