2016

Privacy Awareness in Mobile Business: How Mobile OS and Apps Support Transparency in the Use of Personal Data

Mattis Hartwig
University of Leipzig, hartwig@wifa.uni-leipzig.de

Olaf Reinhold
University of Leipzig, reinhold@wifa.uni-leipzig.de

Rainer Alt
Information Systems Institute University of Leipzig, rainer.alt@uni-leipzig.de

29th Bled eConference

Digital Economy

June 19 - 22, 2016; Bled, Slovenia

Privacy Awareness in Mobile Business:
How Mobile OS and Apps Support Transparency in the Use of Personal Data

Mattis Hartwig

Leipzig University, Germany
hartwig@wifa.uni-leipzig.de

Olaf Reinhold

Leipzig University, Germany
reinhold@wifa.uni-leipzig.de

Rainer Alt

Leipzig University, Germany
rainer.alt@uni-leipzig.de

Abstract
Personal data of consumers has become a highly valuable resource in e-business. Technologies like smartphones, social networks or search engines help to access, collect and monitor an almost infinite amount of data about consumers. In this environment the traditional notice and consent principle seems insufficient for effective privacy protection. Awareness and control are constituting parts of an effective privacy management. This paper investigates how privacy awareness is supported in mobile business. Due to the critical privacy situation in this field, several third-party privacy enhancing mobile apps emerged beside the OS functionalities. The paper explores what information objects these awareness enhancing apps provide. Based on a detailed analysis of 19 apps, a set of 11 information objects is identified that contributes to 4 dimensions of privacy awareness. The findings show that the OS mainly focus on transparency regarding permission systems, that users can obtain more information about the use of their data by using specialized apps and that some dimensions of privacy awareness are almost not supported and open for research as well as the development of new solutions.

Keywords: Mobile Apps, Privacy Awareness, Mobile Business, Privacy Apps

1 Motivation

The amount of data collected and captured increased rapidly in the last few years and will keep rising even faster in the future (Buhl & Müller, 2010). The success of companies like Google Inc. and Facebook Inc. that collect, store and use a massive amount of data illustrates the increasing importance of data as a valuable business asset (Buhl, 2013). In conflict with this growing amount of data used in business processes are the privacy concerns of consumers (Alt, Militzer-Horstmann & Zimmermann, 2015), who start to worry about who has access to their data (Spiekermann, 2012).

In parallel, the technical development of smartphones and the amount of people who own and use a smartphone on a daily basis is also fast increasing (Jin, Yoon & Ji, 2013). Due to its broad applicability, high processing capacity and almost permanent usage, smartphones and their applications (mobile apps) are a suitable tool for gathering personal information about their user (Sutanto et al., 2013). However, the collection and capturing of data is often not transparent, because the existing infrastructure (e.g. IOS, Android) with its monopolized app repositories (Mylonas, Kastania & Gritzalis, 2013) and limited permission systems provide only a minimum of information and influence for the users.

In mobile business, this low trust and rising concerns should be a warning signal as laid out in a study by IPSOS (2012a) where only 55 percent of British Internet users trusted companies with their personal information online and 78 percent of the respondents reported to avoid using specific smartphone apps. The missing transparency of the data use is an important factor as illustrated by a study of the Pew Internet Project on Mobile Privacy and Data Management. The results showed that 30 % of the users had uninstalled an already installed app, due to its collecting of personal information that they did not want to share (Computer & Internet Lawyer, 2012). Another survey has analyzed the 50 most used mobile apps from the iTunes Store and Google Play Store and found that many of these apps transmit data like the phone ID or the current location to the app developer and even to third parties (The Wall Street Journal, 2010). With the increasing presence of multimodal sensors in mobile phones, environmental and user-centric sensor data of unprecedented quantity and quality can be captured from and reported by a possible user base of billions of mobile phone subscribers worldwide (Christin et al., 2011). At the same time, smartphones and tablets are still often poorly secured (Network Security, 2014). A global survey by Accenture shows that 54 percent of the surveyed 1,000 participants worry that using smartphones will erode their privacy (Accenture, 2010).

The current situation calls for a higher privacy awareness, which gives users sufficient information to actively control their privacy level based on their preferences and desired privacy level. This need for more privacy awareness and corresponding knowledge was identified by several app developers who provide privacy enhancing apps that help the consumer to get more privacy relevant information about their mobile phones and the used apps.

The aim of this paper is to provide an overview of the current mobile privacy situation, to analyze what kind of additional information a user can obtain through the usage of privacy enhancing mobile apps and to derive certain fields where the OS provider or other parts in the ecosystem need to adapt in order to enhance the transparency for the user. The research questions of this paper are (R1) What kind of information are available for the user through the usage of privacy applications that are not provided by the OS; (R2) How does this information fit into the dimensions of privacy awareness?

The remainder of this paper is structured as following. In section 2, privacy awareness in the mobile context and the related literature is discussed. Section 3 resumes the work from Au et al. (2011) and compares the three most relevant mobile OS Windows, Android and iOS regarding their privacy handling. Section 4 contains the analysis of privacy enhancing mobile apps first from a broad perspective and then in more detail for the Android OS. Section 5 presents the identified information object that a user can obtain through the usage of privacy enhancing mobile apps and discusses implications for OS and app providers. Section 6 summarizes the key findings and limitations of this paper and suggests directions for future research.

2 Privacy and Mobile Business

In a first step, a literature review about the constituting elements of privacy awareness and the role of mobile Apps and OS was conducted. Following the approach of von Brocke (2009), based on the relevant basic concepts of "Privacy", "Privacy Awareness" and "Mobile Apps" combinations of the key words "privacy", "awareness", "app(s)", "mobile", "permission", "OS" were used for a structured search within the databases Ebsco, IEEE and Google Scholar. In general, only a limited number of papers with relevance for the R1 and R2 was identified and research about mobile apps that support privacy awareness seems scarce. Following Cooper (1988), this literature research helped to identify central issues in existing research outcomes for the presented analysis in this paper.

Clarke (2006) defines privacy as follows: *„Privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations*". Furthermore, privacy can be divided into four interpretations: *Privacy of the Person*, *Privacy of Personal Behavior*, *Privacy of Personal Communications* and *Privacy of Personal Data* (Clarke, 2006). Whereas the last two are maybe heavily harmed by mobile applications.

The general need for more privacy is answered by different approaches, such as Digital Forgetting (Karla, 2010), Privacy by Design (Shapiro, 2010) or Data Property Rights (Lessig, 2006). Current solutions in mobile business often apply so-called privilege or permission systems, but a major issue is the definition of the right amount of permissions. Several researchers work on methods to measure (Geneiatakis et al., 2015) and handle (Han et al., 2014) such privileges. Besides permissions, identity management systems are also discussed as solutions for better privacy protection. Some researchers, such as Enck et al. (2014), also developed technical solutions for analyzing the access and distribution of data to third parties. A study by Mylonas et al. (2013) shows that users often trust official app repositories and that security controls are not enabled or users disregard security during selection and use. The adoption of security and privacy enhancing apps not only increases with negative experiences by users (Okazaki, Li & Hirose, 2009), but also with higher awareness and trust (Han, Wu & Windsor, 2014). In 2011, Passerini (2011) discusses the difficulties of striking a balance between privacy issues and opportunities by mobile tools and apps.

Stach and Mitschang (2013) reviewed android based privacy approaches and conceptualized an own Privacy Management platform. This research was a good basis for this paper but the reviewed approaches where mostly scientific prototypes that focused on hardware and needed a rooted system. Next to those innovative and but rather conceptual approaches there are several app developers who implemented apps that enhance the privacy of the user. The privacy apps from independent providers are more flexible and put the user demand in the center. They also often go further than just fixing the permission problems and introduce new privacy related features such as a risk indicator, virus protection or code analysis for showing what happens with the user data in a broader context. These privacy awareness apps advertise with slogans like "Be a know-it-all to your device's safety with privacy alerts" and "[…] take back control of your privacy!" However, there is still no research analyzing the existing privacy awareness applications, the mobile OS features and the corresponding privacy-related information a user gets and which influences the privacy awareness. Winkler and Rinner (2012) defined four levels of privacy awareness where the privacy level is higher when the user knows more about the system that is a danger to his or her privacy, based on the example of video surveillance. Following this conceptualization of privacy awareness, the user needs to know as much as possible about potential privacy threats. A high level of privacy awareness also requires some sort of warning for the user if new privacy threats come up. Mentioned by Konings et al. (2013) the main approach in privacy management

is often only the control of certain privacy threats but ***privacy awareness*** is a precondition for privacy decision making and therefore for effective privacy management by users or service providers.

The performed literature review provided no concepts or measuring methods for evaluating privacy awareness. However, based on existing research four dimensions for measuring privacy awareness in R2 can be identified (see Figure 1). One dimension is the Permission dimension which is often discussed in the context with smartphones and their permissions to access data (Geneiatakis et al., 2015; Hoffman, 2013). Awareness in this context means, that the user knows what kind of information can theoretically be accessed by certain applications, tools or people. The second dimension is the actual ***Requested Data***. Enck et al (2014) discussed and analyzed this dimension with their TaintDroid app, which analyzes what kind of information is communicated to the outside. The third dimension is ***Consumption***, which deals with the purpose of the data collection. Awareness means that the user knows why the data is collected and how it is used (Cavoukian, 2012). This requirement is also included in the European Privacy Directive. The fourth dimension is ***Self-profiling***. Awareness means that the user knows his own behavior and how it is connected to the other dimensions. The mismatch of the stated interests and the actual behavior is often called privacy paradox and discussed by Norberg et al. (2007).

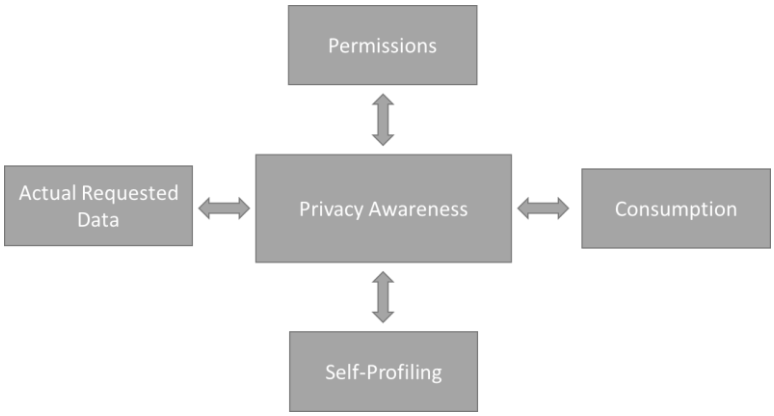

Figure 1: Dimensions of privacy awareness

Winkler and Rinner (2012) included three of these dimensions (without self-profiling) into an examination of awareness levels in the context of video surveillance. The collected data and permission dimension is mentioned in level 0 and 1 where the user gets information about the possibility of video surveillance and the locations where the data is collected. The consumption is addressed in level 2 where the user knows about the purpose of the camera.

The importance of privacy awareness is also recognized by the mobile OS providers. The OS providers constantly update their privacy protection features to meet with market and user requirements, resulting in increases as well decreases of transparency and control. Au et al. (2011) analyzed smartphone permission models of the different operating systems in 2011 and pointed out basic functionalities. More recently Google introduced the new Android 6.0 version where they remodeled their permission system and now offer the user more control. This was also a reaction to the displeasure of many Android users which also resulted in many Privacy Apps violating the marketplace rules that needed a “rooted” android system to give users the control they asked for (Hoffman, 2013). Providers of privacy apps and mobile OS providers are working in parallel to anticipate the privacy demand of users and develop solutions to address that need. OS

providers have the better options for enforcing privacy protection by features or standards, but are also limited by the need to attract app creators that finance the platform and often build their business model around the obtained user data.

3 Privacy handling of different OS

As a first step for answering R1 the functionalities of mobile OS related to privacy awareness are examined. Since Au et al (2011) have already compared different OS with regard to their permission system, their research was used as a basis and enhanced for the purpose of this paper. The analysis of this paper was performed on the three OS: Android, iOS and Windows who together cover a market share of 99,3% (see Table 1). Since Android 6 introduced a brand new permission system, the old and new system are included to highlight the advancement.

Feature \ OS		Android		iOS	Windows 10 mobile
		Android < 6.0	Android 6		
Detail of Permissions /Complexity		High	High	Medium	Medium
Point in time for granting permissions		Installation	Runtime when needed	Runtime when needed	Not specified
Revoking Permissions		Uninstallation of the whole app	For each app and each application possible	Single and global possible	Single and global possible
Awareness features of the OS	Permissions	Detailed permission system and information when installing	Detailed permission system with insight at any time	Medium detailed permission system with some insight at any time	Medium detailed permission system with some insight at any time
	Requested data	None	None	None	None
	Consumption	None	App Developer can explain why he is requesting data in runtime but it is not binding.	Request at runtime and user can only guess about the reason by the situation	Request at runtime and user can only guess about the reason by the situation
	Self-Profiling	None	None	None	None
Available *Awareness Apps* in the respective AppStore		19 Apps that focus on giving information about the privacy status.	16 Apps that focus on giving information about the privacy status	3 Apps that are also available for android (Leo Privacy Guard, My Permissions and Privacy Fix)	None
Available *Control Apps* in the respective AppStore		Apps that hide data, manage passwords, secure VPN-Connections, block advertisements or revoke permissions with rooted system	Apps that hide data, manage password, secure VPN-Connections or block advertisements	Apps that hide data, manage password, secure VPN-Connections or block advertisements	Apps that hide data, manage password, secure VPN-Connections or block advertisements

Table 1: Overview of privacy features in mobile OS

All three OS implement some kind of sandboxing which isolates the apps from each other and the rest of the system (Au et al., 2011). To access certain resources, the app needs a permission, which is handled differently by the OS.

For third-party apps, Android distinguishes between normal permissions like setting the time zone that are automatically granted by the system and dangerous permissions, for example the ability to read the contacts that the user has to grant the app explicitly (Android Developers, 2016). Prior to Android 6, the user had to grant all needed permissions when installing the app. It was a take it or leave it concept where the user could not get anything in between. Being the biggest point of critique of Android's permission system this concept was changed. Android 6 introduced the runtime permission system, which means that users will grant certain permissions when needed. And when they decide not to grant the permission the app is still usable just without the functions that need the permission. The user is also enabled to revoke granted permissions later on which was not possible before and resulted in many rooted systems where workarounds were implemented. Dangerous permissions are packed into groups and if a permission is granted, always the entire group of permissions will be granted.

Apple introduced certain permissions into their iOS that are called during the runtime. Before Android 6 this was a clear advantage for Apple. Some of these permissions can be revoked later on. The biggest problem for iOS is that it still lacks a complete permission system as Android has. First, there is no complete list of permissions the iOS uses and second, the permissions that exist are not as fine-granular as the android permissions and therefore do not give as much information as its competitor.

Microsoft's Windows 10 mobile has the smallest market share of the three OS. The permission system is not as extensive as Android's but the user can grant permissions at runtime and can revoke them later in the privacy settings. Confusingly, some permissions are asked for when installing the app, making this approach a hybrid one.

The improvement of the permission systems from 2011 shows that the critique from Au et al. (2011) and many others (e.g. blog author's, app developer) was fruitful and lead to a change within all three market leaders. Especially the turnaround of the Android OS from being the one with much critique for the permission system to the one with deep transparency methods is a remarkable step. The many third-party apps that offered exactly this level of transparency and control over the permissions in the app store may also have supported that decision. In the context of privacy management, the functionalities from this OS and the functionalities from third-party apps also often complement each other.

Next to the permission system the OS have other characteristics that influence the privacy of the user. Apple and Microsoft have a verification process for the submitted apps which ensures a minimum level of security and correct development whereas Android misses such a process. The high amount of apps in the Android-Store is also influenced by the easy and free publishing process for the app developer. The general technologies and functionalities that are provided by the three OS are very similar which results in similar privacy risks for the user. Examples are the usage of the internet, location-based services communication tools and the like.

The support of the awareness dimensions is quite similar between the OS. Remarkable is that they offer no functionalities for the ***Self-Profiling*** and ***Requested Data*** dimensions. Android below 6.0 offered only little in terms of the ***Permission*** dimension whereas the Android 6.0 offered very detailed information. In the ***Consumption*** dimension, again Android below 6.0 offered no possibility to enhance the awareness, whereas Android 6.0 enables the developer to give optional information about the purpose. In Windows and iOS, the user can only guess and derive a purpose from the point in time at which he or she is asked for granting a permission.

4 Analysis of mobile privacy applications

4.1 Methodology

With Android being the platform with the biggest market share and the platform for which the most privacy apps are available the following analysis focuses on mobile apps for the Android OS. Based on the identified need for information in the four dimensions of privacy awareness, a first key word based search for apps that inform a user about privacy aspects was performed on the Google Play Store. A combination of the following key words was used: “privacy”, “management”, “inspection” and “information”. For the resulting list of apps, an additional backward search was applied by an analysis of the section about related apps to identify additional apps.

From the resulting list, only those apps which focus on informing the user about certain privacy-relevant issues were included into the next step of the analysis. That means security apps which only provide a password functionality or just focus on anti-virus functionalities were excluded. Another criterion was the availability of sufficient descriptions about the functionalities, so that a test could be performed.

Since the research was done over a period of one year the new Android 6 version was released during this time. Because of the big change of the permission management many applications that were based on it got obsolete or had to change. In order to get insights about the impact on mobile apps and changed or new functionalities the search was performed again.

The analysis of the 19 apps included three steps. First, the information in the Google Play Store was analyzed and documented. Second, the app was installed on a mobile device (Samung Galaxy S3). Third, the functionalities of the app were tested and the provided information was documented and crosschecked with the descriptions in the Google Play Store and also if available with the website of the app developer. After these steps, two experts went through the documented information and grouped them into information objects. The grouping itself combined similar pieces of information into one information object. If a piece of information was not fitting into an existing information object, a new one was created. This resulted in 11 different information objects (see columns in Table 2).

4.2 Analysis of mobile applications

Table 2 introduces each analyzed app. It can be observed that most apps have high download numbers (> 100.000) and high user ratings (for detailed information on download numbers, ratings and source links see Appendix I). This supports the assumption that mobile users have an interest in privacy related issues. Therefore, they are looking for apps that promise more insights. Figure 2 provides some examples of how the apps may look on the smartphone when installed.

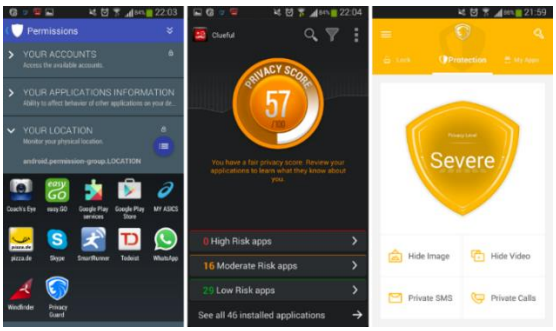

Figure 2: Examples (from left to right aSpotCat, Clueful Privacy Advisor and Leo Privacy Guard)

Information Object / Analyzed mobile Apps		Granted permissions	Risks of permissions	App grouping	Risk of Apps	System privacy level	Privacy related events	Recommendation	Third-party libraries	Social Media Links	Social Media Sharings	Data Value
1	LBE Privacy Guard (06/03/2012, deleted)	X	X				X					
2	Privacy Scanner for Facebook (12/09/2013, deleted)							X				
3	F-Secure App Permissions (30/04/2014, deleted)	X	X									
4	Privatsphäre Monitor (14/11/2013)	X	X	X	X							
5	App Ops (03/02/2014)	X		X			X					
6	Clueful Privacy Advisor (11/05/2014)	X	X	X	X	X						
7	Permission Master – Xposed (05/10/2014)	X										
8	SRT Privacy Inspector (10/10/2014)	X	X	X	X	X			X			
9	PrivacyFix (06/01/2015)							X		X	X	X
10	SnoopWall Privacy App (23/02/2015)	X		X								
11	Privacy Advisor (05/03/2015)	X	X	X								
12	Permission Friendly Apps (21/03/2015)	X	X		X							
13	aSpotCat (24/07/2015)	X	X	X								
14	MyPermissions- Privacy Shield (29/09/2015)	X		X						X		
15	OpenView Mobile - Permission (07/11/2015)	X	X	X			X					
16	Bitdefender Mobile Security & Antivirus (24/12/2015)	X	X		X	X						
17	LEO Privacy Guard (25/01/2016)					X		X				
18	SteelWorks Advanced Permission Manager (27/01/2016)	X	X	X								
19	McAfee App Privacy Advisor (11/01/2016)	X			X			X				

Table 2: Information clusters to which the analyzed mobile apps contribute

The analyzed apps fit with their core functionalities and main purpose into one of the following groups. First, some apps just display the already available information from the Google Play Store in a more convenient and user-friendly way (e.g. aSpotCat). Second, some apps provide additional information and connect with a server where information from different sources is accumulated (e.g. Clueful Privacy Advisor). Third, some

apps have a different stated purpose such as password management but include useful privacy-relevant information as an aside (e.g. Leo Privacy Guard).

Most of the analyzed apps focus on the permissions of the other installed apps. This is due to the restricted permission system for Android < 6.0 apps which follows an “all or nothing”-principle and makes it difficult to find out what permissions an app has after it has been installed. However, besides this permission-related information there are apps with special information objects. All of the identified information objects are presented in the next section (see Table 3).

Despite the fact that some of the permission focused apps like the Clueful Privacy Advisor or aSpotCat have given, also some more information like a risk score for certain permissions, certain applications or the whole system with all its apps, almost no app which has focused on giving information about permissions has been updated after the release of Android 6. On the comment site of the My Permissions – Privacy Shield app at least the developer stated that they are planning for changes accordingly to the new permission system.

5 Privacy related information in Mobile Business

The following section summarizes the results from the OS (section 3) and app analysis (section 4). First, the identified available information objects for privacy awareness are discussed for answering R1. The list of information objects is an artefact that may be used as a reference in further research when analyzing or implementing future apps or OS. Second, the dimensions of privacy awareness from section 2 are reviewed and the support of these dimension through OS and apps is presented for answering R2. The four dimensions together with the mapping of the information objects reveal some shortcomings. Third, possible directions for enhancing the privacy awareness by means of current technologies and research are discussed.

5.1 Information objects

Table 3 presents the identified information objects from section 4 with examples of the type of information that is generated for the user.

The identified information objects show that third-party apps can indeed complement the OS with functionalities that enhance the privacy awareness of the user. For example, some apps visualize the security log so that the user can see what kind of permission was used at what time. Other apps recommend different security setting for specified apps to increase the privacy level. There are also apps that analyze if third-party resources are used, that recognize social media links or that even try to estimate a financial value of shared social data.

Information Object	Description	Example
Granted Permissions	Information about the permissions an individual app has	aSpotCat gives the user information that a certain application has the permission to determine its location.
Risks of Permissions	More information on the single permissions, especially information about the privacy risk of each permission	The Clueful Privacy Advisor tells the user that the permission to read contact details is a permission with medium risk.
App grouping	Grouping of the apps by different factors like functionalities, risk ratings etc.	SteelWorks Advanced Permission Manager can list all applications that can make a direct call to a telephone number.
Risk of Apps	A calculated risk score for single apps based	The Clueful Privacy Advisor tells the user that Whatsapp is an app with a medium risk.
System Privacy Level	An overall privacy score for the whole system of the user	The LEO Privacy Guard gives the user an overall privacy score from zero to 100.
Privacy Related Events	Detailed information about certain privacy relevant actions.	LBE Privacy Guard gives the user information about what app has used what permission at what time. For example Whatsapp determined the location 10 minutes ago.
Recommendations	Recommendations for changes in certain settings either of single app settings, OS settings or even social media settings.	The McAfee App Privacy Advisor recommends the user to change the skype settings so that skype does not use your location.
Third-Party Libraries	Analyses if the apps use certain third-party libraries for marketing or analyzing the user's behavior.	The SRT Privacy Inspector gives the user information what kind of marketing libraries a certain app uses to get the in-app adds.
Social Media Links	Information about mobile apps and known social media platforms and networks.	The MyPermissions- Privacy Shield gives the user information that a certain application has a link with the user's Facebook account.
Social Media Sharings	Information about what kind of data the user shared on social media platforms and who has access to it.	The PrivacyFix App analyzes the information the user posted in certain social networks and shows who has access to it on the basis of the user's settings.
Data Value	Information about the value of certain data that was shared by the user or collected by a third-party app.	The PrivacyFix App calculates a value of the information the user shared in certain social networks. For example, the shared data on Facebook is worth 10 $.

Table 3: Identified information objects

5.2 Support of privacy awareness

The identified information objects can be matched to the privacy dimensions introduced in section 2 (see table 4). The information objects *Privacy Related Events* and Social *Media Sharing* refer to actual data requests or queries and therefore help the user to answer the question what data is actually collected or requested. The information objects *Granted Permissions*, *Risks of Permissions* and *App Grouping* all refer to certain permissions of the apps. These information help the user to understand to which extent an app can access the mobile phone. The information objects *Third-Party Libraries* and *Social Media Links* address the data consumption and possible contacts that can use the data. The information object *Recommendations* gives the user information about what to change in his or her behavior or in his or her settings which is part of the *Self-Profiling* dimension. The *Data Value* also put in the Self-Profiling dimension because its main purpose is to reflect his decisions from an economical perspective but it can also be argued that it is part of the data consumption dimension because it says something of the usage of the data and the value for a third-party player. The remaining two information objects

Risk of Apps and *System Privacy Level* represent aggregated information and can be enhanced by information objects from the other dimensions. However, in the analyzed apps the scores where mainly based on the permission dimension.

	Description	**Matching information objects**
Permission Rights	Summarizes and displays information about the rights that the customer and the service provider (often in form of the app) have in their relationship (e.g. the service provider has the permission to know your location). Provides a structured view of all given permissions with different sorting and search options. Also includes the calculation of certain risk levels and risk scores that allow a benchmarking with other devices or users	• Granted permissions • Risks of permissions • App grouping
Requested Data	Summarizes and displays information about the actual data that is requested or captured by apps and services (e.g. the user's location or the user's contacts). Provides what information the service providers know about the user.	• Privacy related events • Social Media Sharings
Data Consumption	Summarizes information about the actual data consumers (e.g. app providers, third-party advertisers) and about the way they use the data (e.g. for giving location based advertisement). Provides information about potential third-party users and gives information to evaluate the relevance and kind of services they offer. Furthermore gives information about the purposes the data is used for and along with that the effects which certain actions of the user could have.	• Third-party libraries • Social Media Links • (Data Value)
Self-profiling	Summarizes and displays information about the behavior of the user him- or herself. Provides information about possible contradictions between user preferences or statements and actual handling (e.g. the user could say that he or she does not want to share his or her location but installs and uses many apps that require location information). Also gives the user feedback of the value of his or her data.	• Recommendation • Data Value

Table 4: Privacy dimensions and available information objects from apps

The analysis illustrates that the information objects support the different awareness dimensions to a different degree. The permission dimension is covered by many apps which give more detailed information. This was also the dimension which was relatively well-covered by the OS. That indicates that generating information along this dimension a) has a strong demand and b) is possible with the actual technologies. The other dimensions are not that well-covered and have many blind spots for the user. Researchers and developers should put more attention on how to support these dimensions. The nature of these dimensions also calls for the introduction of additional information resources outside the mobile phone, such as service providers that state the purpose of the requested data or monitoring tools that show which marketing services are making use of the provided data. New technologies might also enhance the covering of these dimensions. There are several existing methods for generating additional information future apps or new OS versions could use.

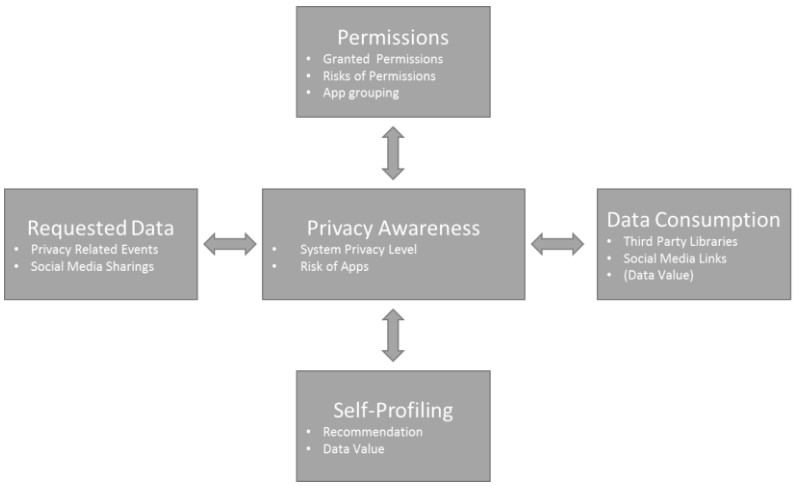

Figure 3: Dimensions of privacy awareness and available information

Regarding the *Self-Profiling*, there are methods for a better assessment of the value of personal data (Feijóo, Gómez-Barroso & Voigt, 2014; Li et al., 2014; OECD, 2013). These methods can be adopted for personal data in the mobile context and implemented in future apps in order to get more and better information about the value of the user's personal data. Letting the user state his disclosure preferences and comparing them with his actual behavior is the key for further improvement of the Self-Profiling. The needed technologies are available and should be used more widely in the future. Regarding the *Data Consumption* more research and collaboration between user and services provider seem necessary. Because it is not possible with the current infrastructure to physically track the personal data along with the whole data consumption, the Data Consumption dimension is difficult to address. One possibility is to include and motivate the service providers to provide information on how the user's data is handled, on why they are using the data and on the involvement and activities of third parties (Domingo-Ferrer et al., 2014). This proactive published information may increase the trust of customers and improve the company image, and can be documented by certificates or seals from third parties that document the following of privacy related rules (Domingo-Ferrer et al., 2014). The *Requested Data* dimension is again difficult to address by the app developer alone. It is necessary to observe which app accessed what information at what time. Furthermore, the communication over all the possible channels needs to be monitored so that the apps cannot share information unnoticed. A general monitoring tool anchored in the OS seems to be the best possible way to do this without giving a third-party app full control over the whole system.

5.3 Directions of app and OS development

During the writing of the paper the version 6 of the Android OS was released, which provides an opportunity to observe the impact on the available privacy enhancing apps. Sufficient information about the permissions were not available at first, afterwards provided by the analyzed apps and finally introduced in the OS itself. The three stages are summarized in Figure 4.

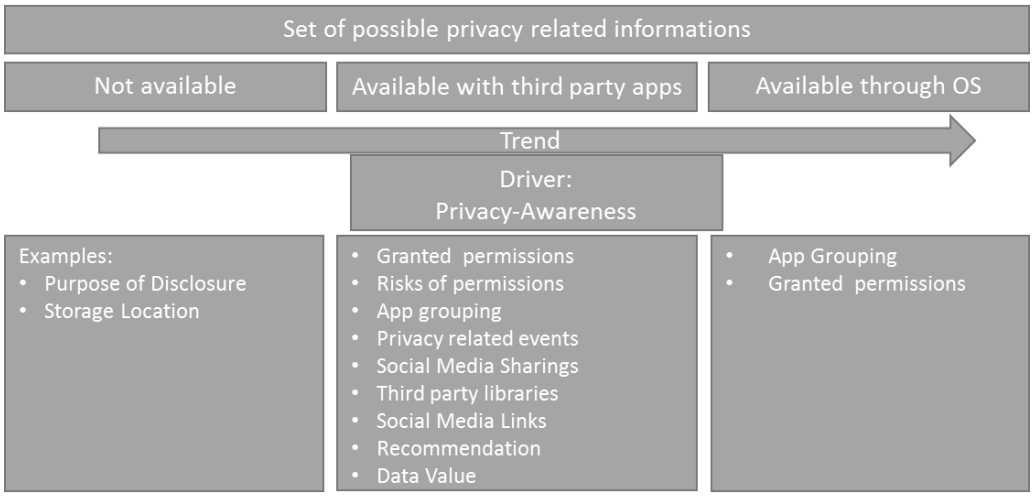

Figure 4: Evaluation stages of the support of privacy awareness

With the release of Android 6, not many apps have changed or new apps were released in the following months. One reason might be the required time for the development in the often community based development groups, but also the still incomplete understanding what functionalities users are looking for to increase their privacy awareness. Most of the providers didn't react on the impact of Android 6 in their app description, only one app provider stated that they are working hard on giving the user functionalities that go beyond the new functionalities of Android 6.

Since the apps and the OS always complement each other with functionalities, the development of the OS itself (see section 3) is also important for the future situation of mobile privacy management. Section 3 illustrates that Android took a big step into the direction of supporting privacy awareness. Together with its very detailed permission system the additional awareness and control features will make the privacy management easier for the user. Windows and iOS are a little bit behind because of the lack of such a detailed permission system, but there are also much less third-party apps that complement the OS features.

6 Conclusions

This research provides a first systematical analysis of privacy related mobile apps and the type of information they provide for users. The high download numbers of the analyzed apps and also the recent developments of the Android OS show the increasing interest of the market and users for such a comprehensive view. The findings show, that following the concept of privacy awareness more information than the permission system of mobile OS is necessary. The performed analysis identified 11 information objects (R1) in four dimensions that contribute to privacy awareness (R2) in mobile business. However, the existing OS and Apps offer only selected information and a comprehensive view is missing. The identified dimensions and information objects provide a first framework for a function based analysis of privacy awareness and may be used as a reference in further research.

The findings also illustrate, that the support of privacy awareness still seems in its infancy and is focused on protecting the user against the apps. The issue of a balance between protection and opportunities in mobile business and the perspective of the service providers is not discussed in detail. With respect to the literature review a lack of interdisciplinary research can be observed. First, many papers focus on technologies that protect the user from giving away data, while research about technologies that support a transparent and consent data use seems to be in the minority. Second, the value

of data and a value based exchange of personal data is not discussed in relation to required technologies and the business value as well as necessity of such data are neglected. Both directions call for more interdisciplinary research, which combines the economic, legal and technological perspectives on privacy awareness and control.

For the development of future privacy awareness functionalities, the findings of this paper provide some insights regarding the necessary information for increasing the transparency. Researchers may use the findings of this research for the investigation of the requirements of privacy awareness and control. Because the insights derive only from the mobile domain, similar studies of desktop apps or social network apps could be performed and used to develop a general concept for information demands of privacy-aware users. A next step of the presented research will be an analysis of the options to increase transparency and how this enhanced transparency can be used to improve control. There are already apps that revoke permission rights and it would be worth exploring how other aspects could be influenced by the user. Supporting systems like coordination platforms for permissions rights or identity management systems may also benefit from more transparency and could be used to monitor the delegation of specific tasks by the users, thus supporting the adoption of such solutions.

Obviously this research has also some limitations. First, only a limited amount of Android apps was examined and more apps should be analyzed to uncover more information objects or to support the identified one. Second, the discussion on new technologies only gives a first direction and an in-depth analysis of current technologies should be performed in a next step. Third, the grouping should be repeated with a larger amount of experts and users to verify the grouping and to add usefulness and requirement dimensions.

References

Accenture (2010). Accenture Newsroom: Use of Smartphones by Bargain-Hunting Consumers is Changing the Customer-Retailer Relationship, Accenture Survey Finds, 13 Apr 2015; http://newsroom.accenture.com/article_display.cfm?article_id=5109.

Alt, R., Militzer-Horstmann, C., Zimmermann, H.-D. (2015). Electronic Markets and Privacy. Electronic Markets, 25(2), pp. 87-90.

Android Developers (2016). System Permissions | Android Developers, 07 Mar 2016; http://developer.android.com/guide/topics/security/permissions.html.

Au, K. W. Y., Zhou, Y. F., Huang, Z., Gill, P., & Lie, D. (2011). Short paper: A Look at SmartPhone Permission Models. In X. Jiang, A. Bhattacharya, P. Dasgupta & W. Enck (Eds.), the 1st ACM workshop: 63.

Brocke, J. v., Simons, A., Niehaves, B., Niehaves, B., Reimer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Research. ECIS 2009 Proceedings.

Buhl, H. U. (2013). IT as Curse and Blessing. Business & Information Systems Engineering, 5(6): 377–381.

Buhl, H. U., & Müller, G. (2010). The “Transparent Citizen” in Web 2.0. Business & Information Systems Engineering, 2(4): 203–206.

Cavoukian, A. (2012). Operationalzing Privacy by Design: A Guide to Implementing Strong Privacy Practices. Ontario, Canada.

Christin, D., Reinhardt, A., Kanhere, S. S., & Hollick, M. (2011). A survey on privacy in mobile participatory sensing applications. Journal of Systems & Software, 84(11): 1928–1946.

Clarke, R. (2006). What's 'Privacy'?, 21 Feb 2016; http://www.roger-clarke.com/DV/Privacy.html.

Computer & Internet Lawyer (2012). Pew Study Sheds Light on App Users' Awareness of Privacy Issues, 29(12): 38–39.

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. Knowledge in Society, 1(1): 104–126.

Document News (2012a). More Consumers Concerned About Companies Sharing Data than Government Surveillance Programmes, 30(5/6): 11.

Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., Schiffner, S., & Danezis, G. (2014). Privacy and data protection by design - from policy to engineering. Heraklion: European Union Agency for Network and Information Security.

Enck, W., Gilbert, P., Han, S., Tendulkar, V., Chun, B.-G., Cox, L. P., Jung, J., McDaniel, P., & Sheth, A. N. (2014). TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. ACM Transactions on Computer Systems, 32(2): 1–29.

Feijóo, C., Gómez-Barroso, J. L., & Voigt, P. (2014). Exploring the economic value of personal information from firms' financial statements. International Journal of Information Management, 34(2): 248–256.

Geneiatakis, D., Fovino, I. N., Kounelis, I., & Stirparo, P. (2015). A Permission verification approach for android mobile applications. Computers & Security, 49: 192–205.

Han, B., Wu, Y., & Windsor, J. (2014). User's Adoption of Free Third-Party Security Apps. Journal of Computer Information Systems, 54(3): 77–86.

Han, W., Fang, Z., Yang, L. T., Pan, G., & Wu, Z. (2014). Collaborative Policy Administration. IEEE Transactions on Parallel and Distributed Systems, 25(2): 498–507.

Hoffman, C. (2013). Android's Permissions System Is Broken and Google Just Made It Worse, 06 Mar 2016; http://www.howtogeek.com/177904/androids-permissions-system-is-broken-and-google-just-made-it-worse/.

IDC: Smartphone OS Market Share, 09 Feb 2016; http://www.idc.com/prodserv/smartphone-os-market-share.jsp.

Jin, B. S., Yoon, S. H., & Ji, Y. G. (2013). Development of a Continuous Usage Model for the Adoption and Continuous Usage of a Smartphone. International Journal of Human-Computer Interaction, 29(9): 563–581.

Karla, J. (2010). Can Web 2.0 Ever Forget? Business & Information Systems Engineering, 2(2): 105–107.

Konings, B., Schaub, F., & Weber, M. (2013). Who, how, and why? Enhancing privacy awareness in Ubiquitous Computing, IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops 2013): 364–367.

Lessig, L. (2006). Code (2nd ed.). New York: Basic Books.

Li, C., Li, D. Y., Miklau, G., & Suciu, D. (2014). A Theory of Pricing Private Data. ACM Transactions on Database Systems, 39(4): 1–28.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34: 47–66.

Network Security (2014). Mobile Security: How to secure, privatize and recover your devices, 2014(2): 4.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. Journal of Consumer Affairs, 41(1): 100–126.

OECD (2013). Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value: OECD Digital Economy Papers.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer Privacy Concerns and Preference for Degree of Regulatory Control. Journal of Advertising, 38(4): 63–77.

Passerini, K. (2011). Privacy in a Wireless World: Issues and Opportunities of Mobile Technologies. Proceedings of the Northeast Business & Economics Association: 385.

Shapiro, S. S. (2010). Privacy by design. Communications of the ACM, 53(6): 27.

Spiekermann, S. (2012). The challenges of privacy by design. Communications of the ACM, 55(7): 38.

Stach, C., & Mitschang, B. (2013). Privacy Management for Mobile Platforms—A Review of Concepts and Approaches, 14th IEEE International Conference on Mobile Data Management (MDM): 305–313.

Sutanto, J., Palme, E., Chuan-Hoo Tan, & Chee Wei Phang (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Quarterly, 37(4): 1141.

The Wall Street Journal (2010). What They Know - Mobile - WSJ, 13 Apr 2015; http://blogs.wsj.com/wtk-mobile/.

Winkler, T., & Rinner, B. (2012). User-centric privacy awareness in video surveillance. Multimedia Systems, 18(2): 99–121.

Appendix

Nr	App	Rating x/5.0	Downloads	URL
1	LBE Privacy Guard	3.0	100,000 – 500,000	(deleted)
2	Privacy Scanner for Facebook	4.3	100,000 – 500,000	(deleted)
3	F-Secure App Permissionn	4.1	100,000 – 500,000	(deleted)
4	Privatsphäre Monitor	4.3	1,000 – 5,000	https://play.google.com/store/apps/details?id=com.think_android.securitymonitor
5	App Ops	3.9	100,000 – 500,000	https://play.google.com/store/apps/details?id=com.findsdk.apppermission&hl=en
6	Clueful Privacy Advisor	4.2	100,000 – 500,000	https://play.google.com/store/apps/details?id=com.bitdefender.clueful&hl=e
7	Permission Master – Xposed	3.8	5,000 – 10,000	https://play.google.com/store/apps/details?id=com.droidmate.permaster&hl=e
8	SRT Privacy Inspector	3.7	10,000 – 50,000	https://play.google.com/store/apps/details?id=de.backessrt.privacyinspector&hl=e
9	PrivacyFix	4.2	1,000,000 – 5,000,000	https://play.google.com/store/apps/details?id=com.avg.privacyfix&hl=e
10	SnoopWall Privacy App	3.9	50,000 – 100,000	https://play.google.com/store/apps/details?id=com.snoopwall.privacyapp&hl=en
11	Privacy Advisor	4.3	5,000 – 10,000	https://play.google.com/store/apps/details?id=com.ashampoo.privacy.advisor
12	Permission Friendly Apps	4.4	100,000 – 500,000	https://play.google.com/store/apps/details?id=org.androidsoft.app.permission&hl=e
13	aSpotCat	4.3	100,000 – 500,000	https://play.google.com/store/apps/details?id=com.a0soft.gphone.aSpotCat&hl=en
14	MyPermissions - Privacy Shield	4.0	100,000 – 500,000	https://play.google.com/store/apps/details?id=com.mypermissions.mypermissions&hl=en
15	OpenView Mobile - Permission Manager	3.3	100,000 – 500,000	https://play.google.com/store/apps/details?id=com.ovmobile.appopslauncher&hl=en
16	Bitdefender Mobile Security & Antivirus	4.4	1,000,000 – 5,000,000	https://play.google.com/store/apps/details?id=com.bitdefender.security&hl=en
17	LEO Privacy Guard	4.3	50,000,000 – 100,000,000	https://play.google.com/store/apps/details?id=com.leo.appmaster&hl=en
18	Advanced Permission Manager – SteelWorks	3.7	100,000 – 500,000	https://play.google.com/store/apps/details?id=com.gmail.heagoo.pmaster&hl=en
19	McAfee App Privacy Advisor	4.4	10.000 – 5.0000	https://play.google.com/store/apps/details?id=com.mcafee.advisory