Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns

Gökhan Bal [a,*], Kai Rannenberg [a], Jason I. Hong [b]

[a] Goethe University Frankfurt, Chair of Mobile Business & Multilateral Security, Theodor-W.-Adorno-Platz 4, 60629 Frankfurt am Main, Germany

[b] Carnegie Mellon University, School of Computer Science, Human-Computer Interaction Institute, 5000 Forbes Ave, Pittsburgh, PA 15213, USA

ARTICLE INFO

Article history:
Received 20 December 2014
Received in revised form
24 March 2015
Accepted 12 April 2015
Available online 22 April 2015

Keywords:
Smartphone privacy
Privacy risk communication
Privacy behavior
Human factors
Experimental research
Information-flow monitoring

ABSTRACT

Modern smartphone platforms offer a multitude of useful features to their users but at the same time they are highly privacy affecting. However, smartphone platforms are not effective in properly communicating privacy risks to their users. Furthermore, common privacy risk communication approaches in smartphone app ecosystems do not consider the actual data-access behavior of individual apps in their risk assessments. Beyond privacy risks such as the leakage of single information (first-order privacy risk), we argue that privacy risk assessments and risk communication should also consider threats to user privacy coming from user-profiling and data-mining capabilities based on the long-term data-access behavior of apps (second-order privacy risk). In this paper, we introduce Styx, a novel privacy risk communication system for Android that provides users with privacy risk information based on the second-order privacy risk perspective. We discuss results from an experimental evaluation of Styx regarding its effectiveness in risk communication and its effects on user perceptions such as privacy concerns and the trustworthiness of a smartphone. Our results suggest that privacy risk information provided by Styx improves the comprehensibility of privacy risk information and helps the users in comparing different apps regarding their privacy properties. The results further suggest that an improved privacy risk communication on smartphones can increase trust towards a smartphone and reduce privacy concern.

1. Introduction

Modern smartphone platforms have unique properties that make them highly privacy-affecting: they are always on, they are connected to the Internet, they follow their users in space and time, they are open to third-party applications (also known as "apps"), and they provide those apps with access to a multiplicity of sensitive resources and information such as location, contacts, call log, or browsing history. Real-world privacy incidents related to smartphone apps such as the "Path" (Thampi, 2012) and "Brightest Flashlight" (Federal

* Corresponding author. Tel.: +49 (69) 798 34702.
E-mail addresses: goekhan.bal@m-chair.de (G. Bal), kai.rannenberg@m-chair.de (K. Rannenberg), jasonh@cs.cmu.edu (J.I. Hong).
http://dx.doi.org/10.1016/j.cose.2015.04.004

Trade Commission, 2013a) cases, where apps transmit highly privacy-sensitive information to their own or to third-party servers without explicitly asking their users for permission, demonstrate the existence of a real threat to user privacy. The presence of such privacy risks notwithstanding, existing privacy notices in smartphone app ecosystems are in most cases not successful in informing users appropriately about potential and actual privacy risks of services. One key explanation for failing in privacy risk communication is that often the underlying conceptualizations of privacy risks are limited to access-control information, such as granting an application access to some resources (e.g. "Application A wants to access your location"). However, such information does not inform users about the risks associated with granting access and, especially in the context of smartphone app usage, relevant factors such as the type of data that is processed, the frequency of access, the destination of sensitive information flows, or the usage of third-party libraries such as ad networks or analytics tools are not considered in risk assessments. We argue that privacy risk assessments of apps should also consider the long-term access behavior of apps, moving from just providing access-control information to also providing privacy-impact information. These kinds of mechanisms should help end-users reason about multiple information flows that happen over time and help them understand the potential and actual impact an app may have on privacy.

In this paper we propose Styx,[1] a privacy-awareness and privacy risk communication system for smartphone platforms. We use privacy-impacting behavioral patterns (PIBP) as the conceptual basis for our system (Bal, 2012). PIBPs are useful for modeling long-term data-access behavior of apps associated with specific threats to user privacy. Thus, the PIBP concept bridges the gap between sensitive information flows and how they impact user privacy. We developed and evaluated a proof-of-concept implementation of Styx to investigate its effectiveness regarding privacy risk communication. We present the results from an experimental evaluation with 50 participants. With our work, we contribute to the knowledge base of information privacy technology design, particularly regarding privacy risk communication methods. More specifically, the contributions of this paper are as follows:

1. We introduce a new perspective and conceptualization for long-term privacy risks of smartphone app usage, that is the *second-order privacy risk* perspective. This second-order privacy risk perspective reflects the potential impact of user-profiling and data-mining on users' privacy.
2. We introduce Styx, a real-time privacy risk communication system for the Android platform that employs the second-order privacy risk perspective.
3. We present results from an experimental evaluation of a proof-of-concept implementation of the user-faced components of Styx to demonstrate its utility, focusing on its effectiveness regarding privacy risk communication.

The paper is structured as follows. Section 2 provides background knowledge by discussing concepts and theories from relevant literature. In Section 3, we discuss our design and evaluation approach in detail. We first present our design principles that we derived from literature on usability aspects of privacy technology. Next, we present the results from the conceptual work behind Styx, i.e. we introduce the central concept and the high-level conceptual architecture of Styx. Following that, we provide details about the design process of the proof-of-concept implementation of Styx, and finally, we provide details and results from the experimental user study that we conducted to investigate on the effectiveness of Styx regarding privacy risk communication. The results of the user study are presented in Section 4. Section 5 first discusses the results of the user study and then discusses potential implications and limitations of our results. Section 6 concludes this article.

2. Theoretical background and related work

In this section, we first emphasize the importance of privacy transparency in privacy protection and provide motivation for focusing on this aspect in the context of smartphone app ecosystems. Next, we discuss the nature of privacy risks in smartphone app usage. We propose a new perspective and conceptualization of privacy risks in the context of smartphone apps and also discuss the causes of these risks. Following that, we discuss existing privacy risk indicators in smartphone app ecosystems and elaborate on their effectiveness. Alternative approaches of privacy risk indicators proposed by other researchers will be discussed subsequently. Finally, we discuss approaches complementary to privacy risk communication systems such as information-flow analyzers and mechanisms that are intended to give users more control over the flow of their personal data.

2.1. *Privacy transparency*

Over the last decades, several international organizations developed basic principles on data protection and codes for fair information processing to foster and guide the protection of individuals' information privacy (European Parliament and Council, 1995; ISO, 2011; OECD, 1980; U.S. Department of Health Education and Welfare, (1973); United States Congress, 1974). Amongst other principles, they all emphasize the importance of transparency (individuals should have a right to view all information that is collected about them). Beyond the general principles for data protection, privacy protection or privacy management can also be described as a process. Derived from Bruce Schneier's (2000) definition of information security as a process, Brunk (2005) proposed the "Privacy Space Framework" that consists of the stages awareness, detection, prevention, response, and recovery. This view on privacy management suggests that privacy management has to start with awareness of privacy-related issues and that without awareness and detection of privacy issues no privacy

[1] Inspired by the river "Styx" in Greek mythology, which formed a boundary between the world of the living and the underworld, around which it flows seven times (The Theoi Project 2014). We use this as a metaphor for our privacy-awareness system that brings sensitive-information flows from the hidden, "dark side" of the smartphone device to the user's "realm".

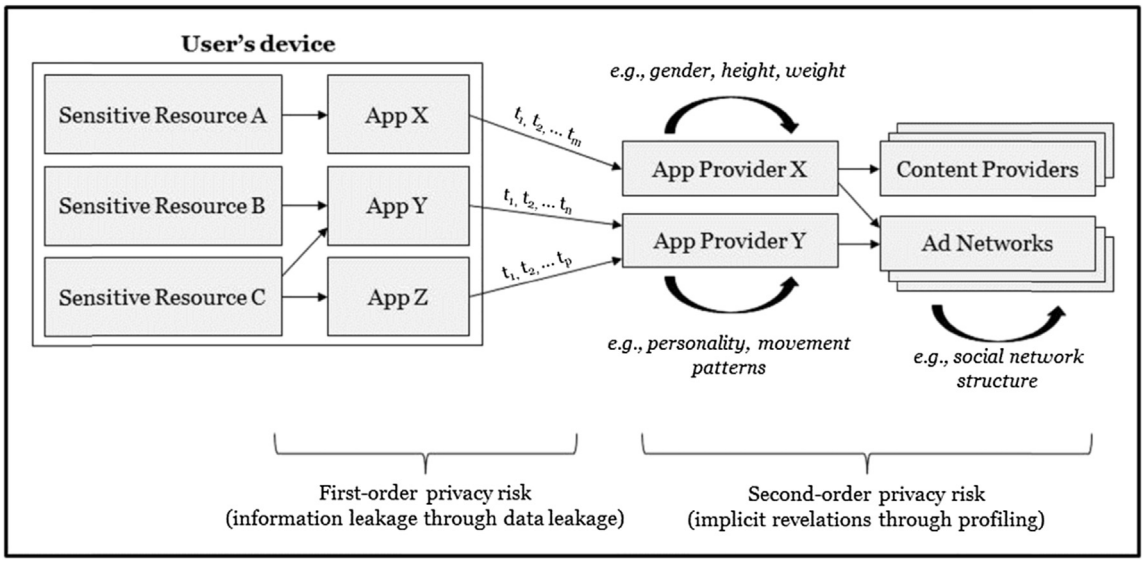

Fig. 1 – First-order and second-order privacy threats of smartphone apps. The privacy risks of smartphone apps are caused by APIs that provide apps with access to sensitive resources. The first-order privacy consequence is leakage of sensitive data. Adding the long-term perspective and risks coming from profiling threats, the second-order privacy consequence is implicit revelation of private information.

management is to be expected. Thus, raising privacy awareness through transparency mechanisms is an essential aspect of privacy protection. We argue that due to the ineffectiveness of privacy risk indicators in smartphone app ecosystems, most users are not aware of the actual extent to which their privacy is impacted by smartphone app usage and that improving transparency is a necessary step in improving privacy protection in this context. Referring to the view on privacy management as a process, we mainly target raising the users' privacy *awareness*. However, we also propose a mechanism to *detect* relevant privacy harming activities of smartphone apps.

2.2. *Privacy risks of smartphone apps*

The harmful consequences of complex technologies are incomprehensible to most people since they are very often delayed or not understood (Slovic, 1987). This finding is also valid for privacy-related consequences of information technology use since privacy-sensitive information flows often happen in the background without the individual's awareness. As a result of the lack of understanding of potential consequences, most people rely on intuitive risk judgments, typically called "risk perceptions" (Slovic, 2000). In order to be effective, risk communication artifacts (e.g. warnings) therefore require proper conceptualizations of the risks in a specific context. Risk assessments can be a useful step for developing intuitive risk communication artifacts such as privacy warnings. The following represents our privacy risk assessment for smartphone app use that informed the design of Styx.

New-generation smartphone platforms such as Android or iOS come with a multitude of technical capabilities that are intended to enable useful services. One particularly important capability is the application programmers' interfaces (APIs) that provide application developers with access to a multiplicity of sensitive resources such as the users' current location, their contact information, camera, call history, or other device sensors. The nature of these types of information makes apps' use of such APIs potentially privacy-affecting since they enable sensitive information flows from the users' devices. Furthermore, access to sensitive resources is not always legitimate or transparent to the users. Two prominent examples of smartphone apps that breached users' privacy are "Path", a social networking app and "Brightest Flashlight". Both apps were found to leak sensitive information without informing the users, and their respective app providers were fined by the U.S. Federal Trade Commission (FTC) for their privacy invasive behavior (Federal Trade Commission, 2013a, 2013b). Several researchers have also analyzed smartphone apps' data-access behaviors. With their dynamic information-flow tracking system TaintDroid, Enck et al. (2010) showed that many apps leak sensitive information without appropriately informing the users. With PiOS, a static information-flow analyzer for the iOS platform, Egele et al. (2011) reported similar results. Consequently, we identify the leakage of sensitive information from the user's device as a first type of privacy risk of smartphone usage.

However, a different kind of privacy risk can be identified when looking at data collection over longer periods. As people use their apps, the quantity of sensitive information they share with app providers and third parties increases over time. When considering dynamic information such as location or browsing history, the privacy threats also increase. Receivers of such sensitive information can build user profiles based on long-term data collected. The potential for using such smartphone-based data to infer new information about users is demonstrated in many data-mining approaches. For example, Kwapisz et al. (2010) showed how collected accelerometer data can be used to uniquely identify the user. Weiss

and Lockhart (2011) showed how the same information can be used to identify user traits such as sex, height, and weight of the user. Min et al. (2013) could infer smartphone users' social network structure by analyzing communication logs on the devices. Similar results are demonstrated by Eagle et al. (2009). The possibility to predict individuals' personality traits by analyzing smartphone usage data has also been demonstrated by Chittaranjan et al. (2011). Further, individuals' movement patterns can be predicted by using smartphone data, as shown by Phithakkitnukoon et al. (2010). The potential for user identification and authentication by analyzing smartphone data has also been demonstrated in numerous studies (Frank et al., 2013; Meng et al., 2013; Owusu et al., 2012; E. Shi et al., 2011; W. Shi et al., 2011; Tey et al., 2013; Zheng et al., 2014). Consequently, we identify a second perspective on privacy risks caused by smartphone apps: *the implicit revelation of private information due to profiling and data-mining capabilities*. Compared to the first type of privacy risks (data leakage), this second perspective applies a long-term view and is more semantics-oriented regarding the privacy breaches, i.e. it better reflects the actual privacy-related consequences regarding private-information revelation. Since the second type of risks is a consequence of the first type, there is a dependency between those two perspectives. To integrate those two perspectives on privacy risks, we introduce the notions of *first-order privacy risks* (data leakage) and *second-order privacy risks* (implicit revelation through profiling capabilities). We want to note that there are more factors that potentially influence the degree of privacy risks such as inter-application communication or sharing with third parties (cf. Fig. 1). In any case, the degree of the second-order privacy threats not only depend on what personal information is shared but also on how frequently personal information is shared in the long run (the long-term data-access behavior).

2.3. Privacy risk communication in smartphone app ecosystems

Privacy indicators and warnings should both motivate users to respond and help them understand the risk of the used services (Bravo-Lillo et al., 2011). Appropriate warnings and indicators should exist in smartphone app ecosystems to help users understand the privacy risks of smartphone apps. In smartphone app markets, one category of privacy risk indicators is privacy policies, in which app providers make statements regarding the processing of sensitive information. However, most users do not read privacy policies due to their complex nature (Milne and Culnan, 2004).

A second category of privacy risk indicator that is specific to the Android platform is install-time permissions. On Android, developers have to declare which sensitive resources their app will access. Before installing an app, users are presented with a list of permissions that the respective app requests. The user then has the choice between accepting or declining all permission requests. In the latter case the installation is aborted. However, researchers have demonstrated that these permission screens are ineffective as a privacy risk indicator. Many users have problems understanding these permissions, because they are vague, confusing, misleading, jargon-filled, and poorly grouped (Kelley et al., 2012). Furthermore, many people ignore the information presented due to an ineffective timing.

In contrast to the install-time approach, the iOS platform uses a run-time permission dialogue. The ineffectiveness of such run-time consent dialogs also lies in the inappropriate timing. Users tend to accept permission requests to continue with their primary tasks (Böhme and Köpsell, 2010). Another potential source of privacy information about apps are the descriptions provided by the app developers. A common practice of some app providers is to explain permission requests in the app description. For example, they justify permission requests by referring to some specific functionality of the app. However, only a few app developers offer such information, and so users cannot rely on them to be provided (Tan et al., 2014). Next, app reviews by other users sometimes consider privacy-related issues. For example, some users make others aware of problematic permission requests when they seem to be inappropriate or unjustified. However, only a few reviews include privacy-related comments (Fu et al., 2013). Furthermore, such information is not standardized, which makes it hard to be identified and to be used for comparing apps. Another source for privacy information about apps are third-party rating portals such as privacygrade.org (Carnegie Mellon University, 2014; Lin et al., 2012, 2014) or checkyourapp.de (TÜV Rheinland, 2014). Those platforms dedicate themselves to providing users with more useful and easier-to-consume information about apps' privacy-related behaviors. They do so by analyzing application code or permission requests and summarizing apps' privacy properties with a rating or with granting a trust seal. While these approaches might be even more useful if they were integrated into application markets, Chia et al. (2012) showed that none of the existing risk signals in smartphone app ecosystems are effective as indicators for the privacy risks and as a consequence, smartphone users rather rely on other trust anchors such as general app ratings or user reviews.

2.4. Alternative privacy indicators

Motivated by the ineffectiveness of existing privacy risk indicators for online services, several researchers designed and developed alternative approaches to improve privacy risk communication. For example, Kelley et al. (2009) used the nutrition-label approach to represent privacy-policy information in a structured way. Another approach used attribution mechanisms to indicate which source (i.e. app) was responsible for a security or privacy-related action on the device, e.g. which app last changed the wallpaper of the device (Thompson et al., 2013). This is intended to support users in identifying privacy-related misbehavior of apps. The approach taken by Lin et al. (2012) to increase the usefulness of Android permissions is to add empirical information about how other users feel about the respective request, e.g. "*95% of users were surprised this app sent their approximate location to mobile ads providers*". Thus, the authors' approach is to model privacy as expectations. Egelman et al. (2009) showed that the timing of privacy notices has a significant impact on the behavior of users. To summarize, the alternative designs for privacy indicators have been shown to have positive effects on the user's behavior, but yet so far there is no approach in

privacy risk communication that employs the second-order privacy threat perspective to consider the long-term data-access behavior of applications and to more accurately reflect how individual apps' behavior impacts user privacy.

2.5. *Information-flow analyzers and control mechanisms*

Complementary to the above approaches for increasing privacy transparency, a separate line of research has sought to systematically analyze smartphone apps regarding their data-access behavior and information-flow characteristics. We believe that privacy risk assessments of apps require in-depth analyses of information flows caused by individual apps. Below, we briefly discuss different categories of analysis techniques for smartphones and also provide references for prominent examples for each of the categories. We also discuss some approaches that are intended to provide users with better control over information flows. Since our research focus is targeted towards improving privacy risk communication, we will not provide a comprehensive discussion about those protection mechanisms. Enck (2011), Amini (2014), and Fang et al. (2014) provide more comprehensive overviews of such techniques in their seminal works.

Information-flow analyzers are tools and techniques to analyze applications regarding the data-access behavior and the sensitive information flows caused by them. The purpose is to identify potential privacy-violating API calls or information flows. Information-flow analyzers can be further classified regarding their techniques employed. Static analyzers look into application binaries or application source codes and determine the potentials for sensitive information flows. Some static analyzers such as PiOS for the iOS platform use control flow analyses on application binaries to determine potential data leakages (Egele et al., 2011), some other static analyzers for the Android platform look into permission requests and permission use by apps. Stowaway is a tool that analyzes permission requests and permission use (Felt et al., 2011). With this tool, the authors detected that about one-third of the applications analyzed are overprivileged, i.e. they possess more privileges than required for the functionality of the app. Kirin is a permission-based privacy and security analyzer for Android apps that look into potentially dangerous combinations of permission requests (Enck et al., 2009). The authors have identified and defined a set of nine potentially dangerous combinations of permissions which is used by Kirin to analyze Android applications. Other information-flow analyzers are AppInspector (Gilbert et al., 2011), SCanDroid (Fuchs and Chaudhuri, 2009), and XManDroid (Bugiel et al., 2011). Except for Kirin, the mentioned approaches have a limited model for the actual privacy risk (first-order privacy risks) since their purpose is more towards detecting data leakages.

Some privacy tools provide the users a more fine-grained or context-sensitive control over their data. Examples are *TISSA* (Zhou et al., 2011), *Apex* (Nauman et al., 2010), *CRePE* (Conti et al., 2010), and *ConUCON* (Bai et al., 2010). Another form of enhanced information flow control for smartphone users is replacing real data with mocked data when apps want to access sensitive resources (Beresford et al., 2011; Hornyack et al., 2011). Analysis results coming from information-flow analyzers can be a useful basis for privacy risk communication, while the improved control mechanisms are more useful when users are aware of the risks. In that sense, all the approaches discussed are complementary to our suggested approach.

3. The design and evaluation of Styx

This section provides details about the design process and the evaluation of our proposed privacy risk communication system for the Android smartphone platform. In Section 3.1.1, we first provide details about the design principles that we identified from existing literature on designing usable security and privacy technologies. We then discuss the key concept behind our proposed privacy risk communication scheme (Section 3.1.2) and introduce the high level architecture of Styx (Section 3.1.3). Finally, we present details and the results of our evaluation of Styx. This includes a partial proof-of-concept implementation (Section 3.2) and an experimental user study that focused on the effectiveness of the privacy risk communication approach (Section 3.3).

3.1. *Designing Styx*

Existing literature on privacy theories and tools provides valuable guidelines for the design of privacy mechanisms and privacy-affecting systems. Our requirements analysis for Styx resulted in a set of principles that we discuss in the following.

3.1.1. *Design principles*

3.1.1.1. Design principle 1: communicate the existence of a threat. To motivate users to make use of privacy protection mechanisms or to perform privacy-respecting behavior, they must believe that their assets (personal data) are under threat, and that the security mechanism provides effective protection against that threat (Sasse and Flechais, 2005). The existence of a threat to their privacy should be communicated to users.

3.1.1.2. Design principle 2: Do not obscure actual and potential information flow. Lederer et al. (2004) describe five pitfalls in the design for privacy. Two of those pitfalls concern the users' understanding of privacy risks: obscuring (1) actual and (2) potential information flow. The authors argue that "designs should not obscure the nature and extent of a system's potential for disclosure" and they "should not conceal the actual disclosure of information through a system". "Users can make informed use of a system only when they understand the scope of its privacy implications". For our purposes, we summarize these two pitfalls in the design principle that actual and potential information flows should be made transparent to the users.

3.1.1.3. Design principle 3: Make potential privacy consequences explicit. Warning science suggests that more explicit communication of risks and consequences can increase the effectiveness of warnings and promote informed decision-making (Laughery et al., 1993). We adopt this same idea for privacy risk communication.

3.1.1.4. *Design principle 4: Consider second-order privacy risks.* Privacy threats go beyond the leakage of single pieces of private information. As discussed in Section 2.2, a different perspective on the threats to information privacy is the implicit revelation of private information through profiling potentials (second-order privacy risks). A similar concept has been defined by Brunk (2005) with the term "exoinformation". It describes those types of information that can be built by "piecing together" what has been collected about a user. Communicating second-order privacy risks, or exoinformation, will give users with a more accurate perception of what they reveal about themselves when using privacy-affecting services.

3.1.1.5. *Design principle 5: Minimal distraction/filter information.* This principle emerges from the character of privacy tools being secondary tasks, i.e. they are always accompanying a primary task. If privacy-related information (e.g. privacy notices or informed-consent dialogs) occur too frequently, the users might feel disturbed from their primary tasks and as a consequence ignore the privacy information. Consequently, the frequency of risk communication should be minimized. The criterion of minimal distraction has been defined by Friedman et al. (2002) in the context of informed-consent dialogues for the Mozilla web browser. A privacy management system should filter information and alert users only to potentially important or new concerns and threats (Goecks and Mynatt, 2005).

3.1.1.6. *Design principle 6: avoid the use of privacy jargons.* One of the major reasons for the ineffectiveness of privacy risk indicators is the use of jargon that cannot be understood by non-experts. As such, privacy risk communication methods should aim to use simple language (Cranor, 2005).

3.1.1.7. *Design principle 7: provide meaningful summaries of privacy information.* Users appreciate short summaries, as long as these summaries do not hide critical information. Standardized formats allow them to find the information of most interest quickly (Cranor, 2005).

3.1.1.8. *Design principle 8: Provide educational opportunities to users.* Privacy notices should not solely inform users about current privacy threats or breaches. They should also fulfill the function of educating users to foster privacy-respecting behavior in future. Also, users are interested in learning more about privacy through time (Cranor, 2005). Privacy notices should therefore also include such educational features.

3.1.2. *Key concept: privacy-impacting behavioral patterns*

As the conceptual basis for Styx we use privacy-impacting behavioral patterns (Bal, 2012). Privacy-impacting behavioral patterns (PIBP) draw on the concept of second-order privacy risks. As discussed in Section 2.3, the common approach for privacy notices implemented by the major smartphone platforms is to inform users about single, potentially privacy-impacting, information flows (e.g. permission requests on Android, run-time consent dialogs on iOS). In this case, privacy risks are modeled as single data leakages (simple example: "Application A wants to access your location"). The assumption here is that consumers are able to map that specific information-flow instance to the impact it will have on their privacy. However, this information-flow level approach does not consider long-term aspects such as frequency of access or combinations with information flows of other type. Location information, for example is dynamic. A one-time access to the resource will not exploit the full potential of knowledge extraction. But, the more often an app accesses the user's current location, the more information can be inferred about the user. An app that accesses the user's location every 30 min could infer where the user lives, where he works or goes to school, which locations he visits in his leisure time, and so on. In this case, the specific PIBP would be "accessing geolocation every 30 min or more often". One could think of more complex examples where different sensitive resources are combined. Privacy-impacting behavioral patterns of smartphone apps are a means to formulate certain privacy-impacting data-access behavior of apps that relate to specific privacy risks such as the implicit revelation of private information due to profiling and data-mining capabilities (cf. Fig. 2).

3.1.3. *Styx architecture*

In this section we present the conceptual architecture of Styx, a PIBP-implementing privacy risk communication system for the Android platform. We do not provide a complete implementation of Styx, since our focus is primarily on the user-facing parts, namely the risk communication features and their effects on user perceptions regarding the risks. Our purpose of presenting a complete high-level architecture is to guide potential implementations. The high-level architecture of Styx, including its components is illustrated in Fig. 3.

Styx Monitoring. A monitoring of sensitive information flows is essential for assessing the long-term privacy impacts of an apps data-access behavior. This component is responsible for dynamically monitoring sensitive information flows between the device and applications. It could be triggered by API calls of apps to access sensitive resources. The sensitive resources to be monitored have to be defined upfront. Such a component requires an extension to the Android framework (the white component in the Android OS Permission Check in Fig. 3). Existing dynamic information-flow analyzers such as TaintDroid (Enck et al., 2010) can be a useful basis for the monitoring component.

Styx Log. This component is a database storing information about sensitive-information flows observed by the monitoring component. The purpose of the log is to create a history of data-access triggered by apps, which can be used by the other components to assess the privacy-related properties of individual apps. Keeping a history of information flows is essential since the privacy-invasiveness of an app is also determined by past data accesses.

Styx Pattern Collection. Styx models privacy impacts as behavioral patterns of apps (second-order privacy risks). Therefore, Styx must have access to a set of such privacy-impacting behavioral patterns to match applications' data-access behavior with pre-defined behavioral patterns. Three exemplary patterns were presented in Section 3.1.2. Those patterns are stored in the pattern collection database. A data format similar to policies must be defined to have a standardized data structure.

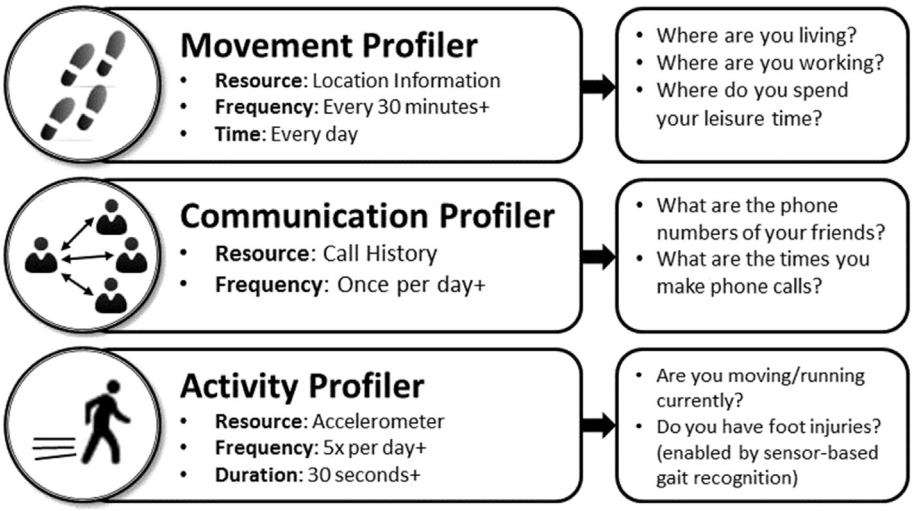

Fig. 2 – Example privacy-impacting behavioral patterns. Source: (Bal, 2012). The figure shows three examples of privacy-impacting behavioral patterns (left part) with respective information that the user potentially reveals as a consequence (right part). Each pattern comes with a description of the access behavior, including information about the accessed resources and the temporal aspects such as frequency of access, time of access, and duration.

Styx Pattern Detection. The actual matching between observed app behavior and PIBPs is performed by this component. It is triggered by the monitoring component after a new entry has been stored in the log. The pattern detection mechanism then takes the Styx Log (including the new entry) and the pattern collection as input and tries to match patterns with application behavior.

Styx Notification. This component is responsible for notifying the user about matches that have been identified by the pattern detection. Ultimately, this is the user-facing

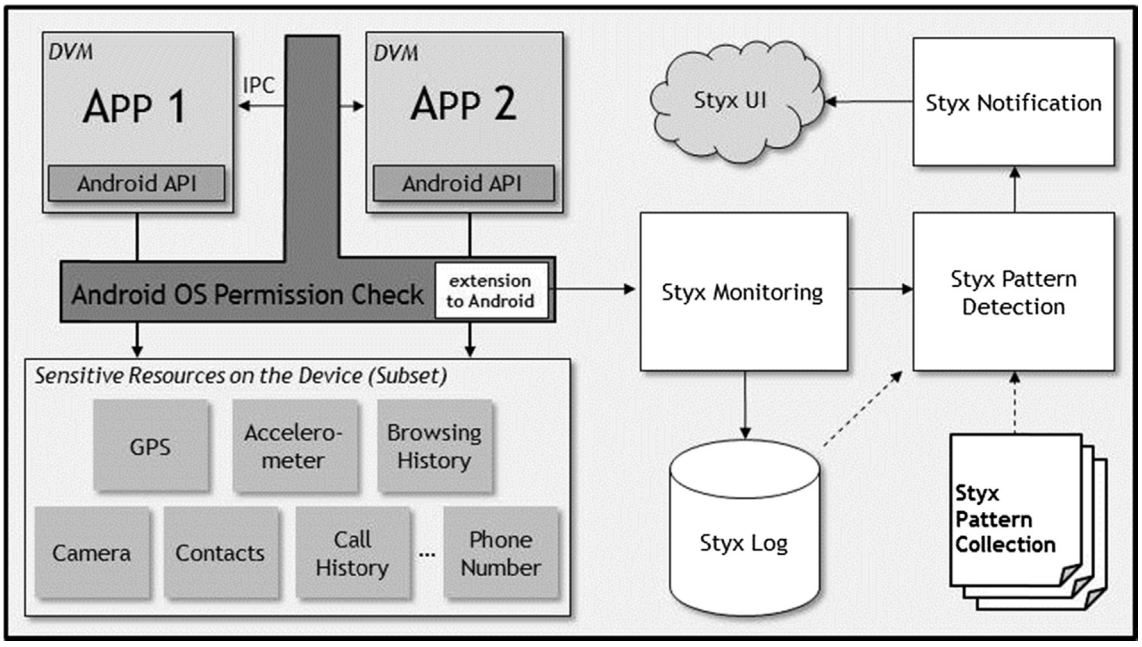

Fig. 3 – Conceptual Architecture of Styx. Android's permission-based security architecture is sketched on the left-hand side of the figure. Styx requires an extension to the Android framework and a listener located at the permission-check mechanism (white box in the Android Permission Check). The main components of the Styx architecture are presented on the right-hand side of the figure. The main Styx mechanisms are the Styx Monitoring, the Styx Pattern Detection, and the Styx Notification components. The data sources of the Styx mechanisms are the information-flow history of apps (Styx Log) and a set of pre-defined data-access behavior patterns (Styx Pattern Collection). The Styx UI is the user facing component of Styx.

component of the system and therefore its design is of key importance. It uses the notification mechanisms of the smartphone platform to show the Styx UI to the user. The UI will present information about privacy-impacting behavior of the respective app and the consequences regarding user privacy.

3.2. *Proof-of-concept implementation of Styx*

3.2.1. *Design process*

We implemented a proof-of-concept of Styx for the purpose of evaluating its effectiveness. As stated in the beginning of this paper, Styx ultimately aims at improving privacy transparency and individuals' privacy awareness. Consequently, we focused our implementation on the user-facing part of the architecture, namely the notification component and its respective user interfaces. The Styx monitoring, logging, and pattern detection mechanisms are simulated in our proof of concept. For the purpose of the user study, we inspected the permissions requested by some apps that we used in our study and used our expert knowledge and results from data-mining literature (cf. Section 2.2) to come up with a small set of simple PIBPs and personal information that users would implicitly reveal to the app providers (second-order privacy risk). Example information are "your hometown", "your home address", "your daily movement patterns", "your favorite points of interests" (all based on different access-patterns to location information), or "your close friends", "your phone call behavior" (based on communication logs). We then applied a two-step, iterative design approach with pre-tests to develop and improve the Styx user interfaces. In a focus-group approach, the first iteration of Styx was shown to nine colleagues at Goethe University Frankfurt. For each screen, the participants were asked to answer the following questions: "What is the intention of this screen?", What actions have you performed? Why?", "Did you find any bugs? Please report.", and "Suggestions for improvements?" In the next design iteration, another five people were given the same tasks. The third version of Styx was then used in the experimental user study. This experimental version of Styx is composed of six different screens that represent different types and levels of privacy information. The respective purposes of the screens are described in the following.

1. **Styx Notification**. The notification entry in the notification menu is the first user interface that is presented to the users. It provides a short summary of a privacy-impacting behavior of a specific app. The app's name and the potential information leakage is mentioned in the notification. Furthermore, there is a graphical representation of the private information (a. in Fig. 4).
2. **Styx Inference Screen**. This is the landing page of Styx after the user clicks on a notification entry. The purpose is to visually communicate what private information the user has implicitly revealed to the app provider. In the simple example in Fig. 4b) it's the user's gender.
3. **Styx Rating**. This screen (cf. Fig. 4c) is intended to help users understand whether the application's behavior is unusual or rather something expected. Factors that influence this rating are the functionality of the app and also a comparison with apps of the same category (e.g., "Are similar apps also able to determine the user's gender?"). The classifications are as follows: "very usual", "usual", "unusual", and "very unusual".
4. **Styx Basis Screen**. To make the underlying mechanisms of Styx transparent to the user, we also provide information about the respective privacy-impacting behavior of the app (i.e., which resources did it access in what manner?). The users will be able to better understand the relation between concrete privacy impacts and access to sensitive information. In the example in Fig. 4d), the app has accessed the list of installed applications and is able to see the high number of sports-related apps on the device.
5. **Styx Detailed Pattern Information**. In its approach to provide on-demand access to more detailed information, Styx shows the users more detailed information when they clicks on the "Read more … " part of the inference screen (Fig. 4e).
6. **Styx Dashboard**. This screen is essential to communicate the overall privacy-invasiveness of an application. It summarizes what other identity-related information the current app could potentially infer based on past information flows. Each information item can be clicked on to open the detailed information screens. The goal was to make this screen very concise, intuitive, and visually attractive. The Styx Dashboard plays an important role in enabling the comparison of privacy-related properties of different apps (f. in Fig. 4). Its design is influenced by location-based gamification approaches such as "Foursquare", in which the users can "unlock" certain achievements when matching some usage behavior (e.g. "visiting five different restaurants within one week"). In Styx, the icons represent "unlocks" of apps regarding personal information. Thus, compared to the gamification approaches, they represent "negative" unlocks from the user's perspective.

3.2.2. *Meeting the requirements*

Styx is primarily intended as a privacy risk communication system, thus its focus is to communicate the users the existence of privacy-related threats (Design Principle 1). Styx further keeps track of all sensitive-information flows and considers them dynamically in its risk assessment mechanisms. Therefore, actual and potential information flows are not obscured, but rather considered in the risk assessments (Design Principle 2). By employing the second-order privacy risk perspective (Design Principle 3), the privacy risks are made more explicit to the users (Design Principle 4). Another advantage of the behavior-pattern based approach is that privacy-related notices only occur when a certain behavior pattern is matched instead of informing per information flow. This provides a good basis for minimally distracting the users through filtering information (Design Principle 5). In our proof-of-concept implementation of Styx, we avoided the use of privacy jargon. With a two-round pre-test evaluation approach, we assured that the wording used in Styx is understandable to a general audience (Design Principle 6). The Styx Dashboard is intended as a user interface summarizing the privacy-related properties of individual apps (Design

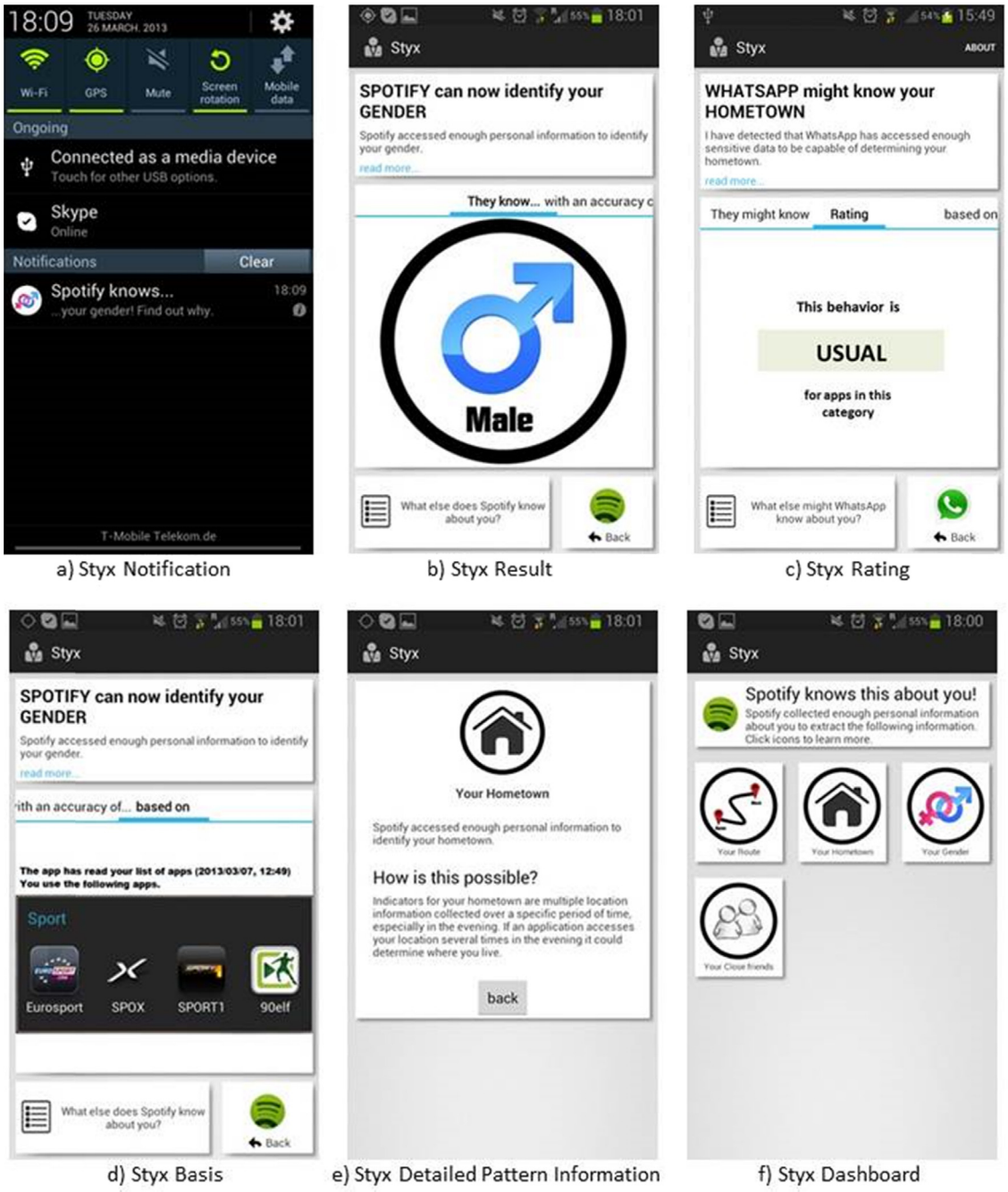

Fig. 4 – Screenshots of the proof-of-concept version of Styx. a) shows the notification entry that briefly informs the user about a new privacy-related event, b) shows the "result screen" that shows what personal information the app can infer about the user based on its data-access behavior, c) shows the "Rating Screen" that is intended to help users understand whether the application's behavior is unusual or rather something expected, d) shows the "Basis Screen" that communicates the respective data-access behavior (in the example, the app has accessed the user's list of installed applications), e) presents detailed information about a specific pattern matching, and f) shows the "Dashboard" that summarizes an app's privacy-invasiveness based on past data-access behavior.

Principle 7). The "Basis" screen of Styx is intended as providing educational opportunities to users (Design Principle 8). It explains why some personal information might have leaked by referring to the respective privacy-impacting behavior of the apps.

3.3. *Evaluation of Styx in an experimental user study*

The ultimate goal of our research was to investigate more effective approaches for privacy risk communication on smartphone platforms. Thus, the focus of our evaluation of

Styx is on its user-facing parts that are relevant for risk communication and how they influence user perceptions such as comprehensibility, privacy concerns, and trust. We therefore decided to conduct experimental user studies in which we compared the effectiveness of Styx as a privacy risk communication tool against the state of the art (i.e. permission request screens). Experimental user studies are a very useful method to investigate how newly developed artifacts such as privacy warnings influence their environment (e.g. user perceptions and behavior). As a measure for effectiveness, we designed and used questionnaires that the participants of our study had to complete during the experiments. The questionnaires asked questions related to the comprehensibility of privacy risk information or how trustworthy the experimental smartphone was perceived. We conducted our experimental user study in spring of 2013 in the user study labs at Carnegie Mellon University. Participants were recruited through the CBDR Participant Portal of the university, which is an online system that help researchers in organizing their user studies. We invited people to a "User Study about Smartphone Apps" without mentioning the topic of privacy in the advertisement. The prerequisites were that the participants should be at least 18 years old and have experiences with the Android smartphone platform. Participants were compensated with a $10 gift card for an online shop for their time. Prior to starting with the user study, it was given approval by the university's Institutional Review Board (IRB).

3.3.1. *Participants*

In total, 77 participants registered for the study, out of which 50 showed up during the two-week experiment phase. 18 of the participants were female (36%), 32 were male (64%). The average age of the participants was $M_{age} = 25.56$ ($SD = 7.18$). 27 of the participants had permanent residence in the U.S. (54%), 23 had permanent residence in another country (46%). 2% of the participants owned a smartphone for less than 1 month, 6% for 1–3 months, 20% for 3–12 months, 14% for 1–2 years, 26% for 2–3 years, 8% for 3–4 years, and 24% for more than 4 years. In average, the participants had installed $M = 25.54$ apps ($SD = 25.32$) on their own devices and used in average $M = 9.12$ apps regularly (at least once a week; $SD = 7.13$).

3.3.2. *Experimental design*

The experiments have been conducted in the labs of the Human–Computer Interaction Institute at Carnegie Mellon University. We invited one participant at a time to take part in the 1-h experiment. Since our main goal was investigating the second-order privacy risk communication approach against the more common first-order privacy risk communication approach, we used a between-subjects design for the experiment. Before starting the experiment, participants were randomly assigned to one of the two conditions (FO-PRC: first-order privacy risk communication or SO-PRC: second-order privacy risk communication). They then had to read a consent form on the lab computer and agree to the conditions described if they wanted to take part in the experiment. Next, we handed them the experimental smartphone (Samsung Galaxy S3 LTE) on which Styx was installed and running in the background.

After introducing the participants to the key UI concepts of the device, we handed them an instruction sheet containing a step-by-step description of what they should do with the device during the experiment. The tasks were about starting specific apps and using some of their core features. We used six types of apps during the experiment: to-do list manager, favorite TV show manager, weather forecast, dice, flashlight, running tracker, and a memory game for kids. The instruction sheet explicitly told the participants what to do (e.g., "Start the GTasks app", "Add a new note by pressing the +-symbol", "Press the back button to see the list of notes", "mark your note as checked", etc.). In pre-defined points in time unknown to the participants, the device showed notifications in the notification bar and played an alert sound. Participants in the SO-PRC condition were shown the Styx privacy user interfaces with second-order privacy risk information, and participants in the FO-PRC condition were shown a chronologically ordered information-flow history (cf. Fig. 5). The participants were free to examine the notifications. Only in the case of the weather (third app) and the running app (sixth app) we explicitly instructed them to examine the notification and the respective user interfaces. After the participants finished the smartphone tasks, they were asked to complete the questionnaire on the lab computer.

3.3.3. *Collected data*

During the experiments, we collected a variety of data that would allow us to evaluate the effectiveness of Styx according to our evaluation targets while the main goal was evaluating the new privacy risk communication method regarding its effectiveness in privacy risk communication. We collected data by means of a questionnaire (cf. Appendix) that contained question items to measure various constructs related to the effectiveness of the proposed privacy risk communication approach. We were interested in how comprehensible the Styx privacy information was perceived by the participants. We therefore included a *comprehensibility* scale to the questionnaire. This scale consists of three question items (Cronbach's Alpha[2] = .823; example item: "The privacy information that have been presented on this smartphone were easy to understand"). Another aspect we were interested in was regarding how the new type of privacy risk communication affects individuals' privacy concerns regarding smartphone apps and also how it affects people's perceptions regarding the trustworthiness of the smartphone device with such a privacy-awareness system. We therefore included a self-developed 6-item scale for measuring *privacy concerns with smartphone apps* (Cronbach's Alpha = .937; example item: "For me, it is important to know which personal data are accessed by my apps") and a self-developed 4-item scale for measuring *trust in the smartphone device* regarding the protection of users' privacy (Cronbach's Alpha = .726; example item: "This

[2] Cronbach's Alpha is an estimate of the reliability of a psychometric test (e.g. an instrument for measuring a specific latent variable such as comprehensibility of privacy information).

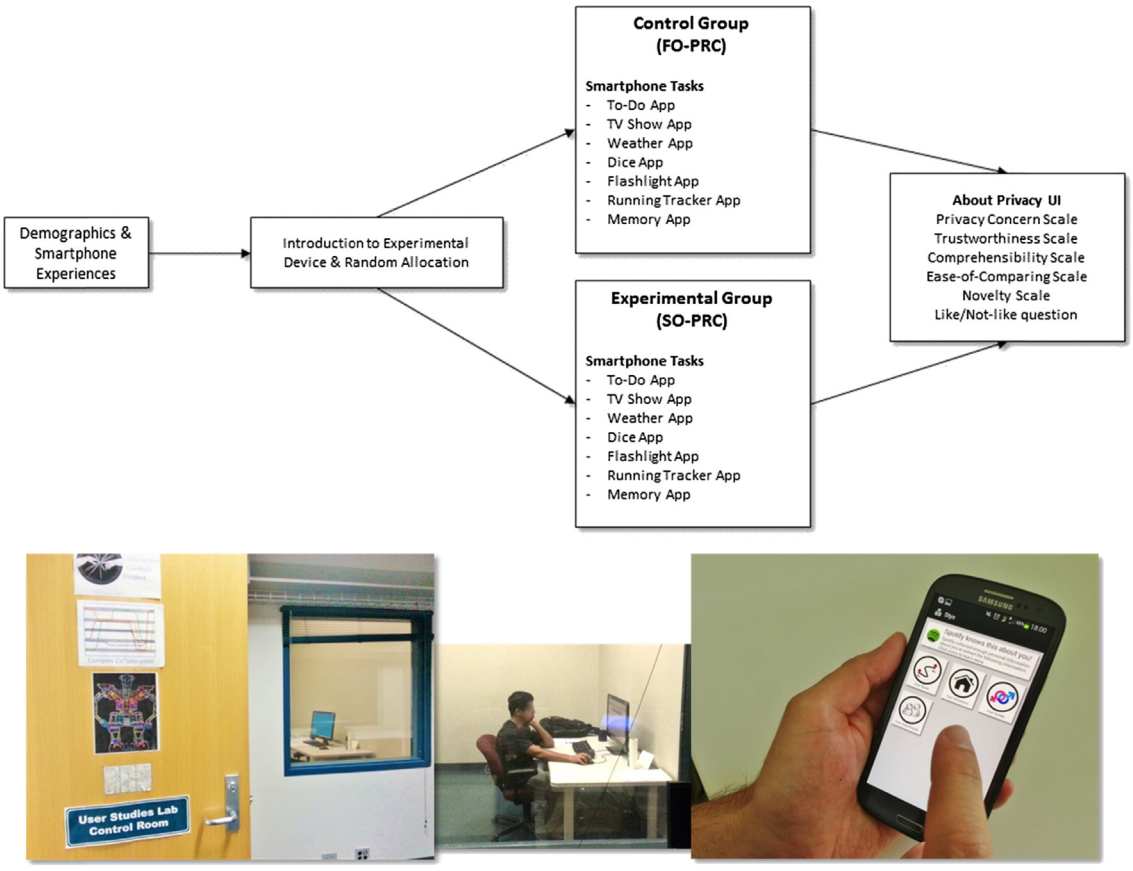

Fig. 5 – Experimental procedure (top) and user study control room (bottom). Participants took part in 1-h experiments in the user studies lab in the Human–Computer Interaction Institute at Carnegie Mellon University. Participants completed questionnaires on the lab computer and performed tasks on a lab smartphone as instructed on a sheet.

smartphone supports the user in identifying potential misuse of personal data by apps").

Two important features a privacy risk communication system should fulfill are to help users understand (a) the degree to which an app invades users' privacy and (b) compare different apps easily regarding their privacy-related properties. We therefore added a 2-item scale adapted from Kelley et al. (2009) to measure the *ease and enjoyment of comparing apps* regarding their privacy properties (Cronbach's Alpha = .916; example item: "With this privacy user interface, it is easy to compare different apps regarding their privacy friendliness"). We further proposed Styx as an innovative approach to communicate privacy risks of smartphone apps. To assess *perceived novelty*, we used the respective scale from the User Experience Questionnaire (Laugwitz et al., 2006). Participants had to complete the questionnaire after the experiment on a computer in the lab. All items were rated on a 6-point Likert scale ranging from "strongly disagree" to "strongly agree". When testing new user interfaces, it's particularly helpful to also ask participants open questions to gain insight into potential problems and misconceptions of the system. As part of the evaluation we therefore asked the participants in the questionnaire what they particularly liked and did not like about the new privacy user interface. They could enter up to five aspects per question into open text fields.

4. Results and findings

In our statistical data analyses, we used non-parametric tests since normality tests on our data revealed that they are significantly non-normal. Thus, the assumptions for using parametric tests are not met and non-parametric tests would provide more accurate results in this case. To compare the mean values of our scales in the two conditions, we applied the non-parametric Mann–Whitney U test to the scales. The first nine data sets were removed from the data analysis to protect the internal validity of the study since changes to the prototype were introduced after the first day of the experiments. The total size of the remaining population was N = 41. The FO-PRC group had a size of $n_{no\text{-}prc} = 19$ participants, the SO-PRC group had a size of $n_{so\text{-}prc} = 22$ participants. The results of the Mann–Whitney U tests are summarized in Table 1. The perceived comprehensibility of privacy information had a mean rank of 19.50 in the FO-PRC condition and 22.30 in the SO-PRC condition. The difference is statistically not significant. The ease-of-comparing scale shows a mean

Table 1 – Results of Mann–Whitney U Tests; *p < .05. In this non-parametric test, all mean values per participant across all experimental conditions are brought into an ascending order (rank). The test then calculates the mean ranks of each condition and calculates whether the difference in the mean values are statistically significant. The table shows the mean rank values for each scale and experimental condition, the result of the test statistics (*U*), the standardized test statistics (*z*), the significance level (*sig.*), and the effect size (*r*).

Scale	Mean rank (N = 41)		*U*	z	*sig.*	*r*
	Control (FO-PRC)	Experimental (SO-PRC)				
Perceived Comprehensibility	19.50	22.30	180.50	−.75	.231	−.12
Ease of Comparing	18.55	23.11	162.50	−1.25	.108	−.20
Smartphone Privacy Concern*	24.50	17.98	142.50	−1.79	.037	−.28
Trust Smartphone	18.42	23.23	160.00	−1.29	.102	−.20
Perceived Novelty*	16.74	24.68	128.00	−2.13	.017	−.33

rank of 18.55 in the FO-PRC condition and 23.11 in the SO-PRC condition. The difference in the mean ranks is statistically not significant. Privacy concerns with smartphone apps showed a mean rank of 24.50 in the FO-PRC condition and 17.98 in the SO-PRC condition. The difference in the mean ranks is statistically significant ($p < .05$). The trustworthiness of the smartphone scale shows a mean rank of 18.42 in the FO-PRC condition and 23.23 in the SO-PRC condition. The difference is statistically not significant. Finally, the perceived novelty of the privacy user interfaces shows a mean rank of 16.74 in the FO-PRC condition and 24.68 in the SO-PRC condition. The difference in the mean ranks is statistically significant ($p < .05$).

Regarding the responses to the question "what did you *not* like about the privacy user interface?", we focus our analysis on the responses of the participants in the SO-PRC condition. Four responses were related to the comprehensibility of the information (example answer: "It just took some time to figure out what Styx was about."). Eight responses on the other hand were about how annoying the notifications were during the experiment (example answer: "I disliked the constant notification"). Three responses were about the usability of the UI (example answer: "I also did not like the graphical interface"). Nine responses were about some functionality that participants would additionally expect (example answers: "I would have loved if the app could suggest me another app with same functionality but lesser data access", "It should pop up before the app starts sending data"). Looking at the responses to the question "what *did* you like about the privacy user interface?", there were noticeably more responses that refer to the comprehensibility and usability of the UI. In total, 13 responses can be classified as such (example answers: "The notifications were self-explanatory", "The notifications covered all the information regarding the app using personal info in brief sentences"). Nine responses can be classified as relating to the usefulness or the perceived purpose of the privacy user interfaces (example answers: "I liked that I could see a list of these icons and use that list to compare one app to another", "I liked the icons categorizing the types of data that Styx detected"). In sum, the analysis of the data revealed some existing issues with Styx (e.g. people expect additional information or instructions on what to do next), some of them being caused by the experimental design, however, regarding the comprehension and usefulness of the privacy user interfaces, Styx was quite successful in achieving its goals.

5. Discussion

The data analysis revealed that all in all Styx as a second-order privacy risk communication system is successful in improving privacy risk communication. Even though not statistically significant, participants in the SO-PRC condition found the privacy information presented more comprehensible than participants in the FO-PRC condition. Also, they found it easier to compare different apps regarding their privacy-related properties. Particularly interesting is that there was also a statistically significant difference in the privacy concerns regarding the smartphone apps and potential leakage of sensitive information. Participants in the FO-PRC condition had significantly higher privacy concerns compared to participants in the SO-PRC. This is an indication for the success of Styx in more accurately communicating the privacy-related properties of apps. Participants in the FO-PRC condition might have been biased by the pure length of the information flow history without actually understanding the degree to which their privacy was affected. Thus, communicating the second-order privacy risks seems to help people in better understanding the actual degree of the risks. A similar observation can be made regarding the perceived trustworthiness of the smartphone used in the experiment. Participants in the SO-PRC condition had higher trust in the smartphone platform to protect their privacy against harmful apps. Thus, the improved privacy risk communication system positively influenced the overall trustworthiness of the device. Finally, participants in the SO-PRC condition recognized Styx as an innovative approach to communicate privacy information. The differences in the mean ranks between the two groups were statistically significant.

The responses to the open text questions regarding what the participants particularly liked and not liked further helped us to identify existing problems with our Styx implementation but also to identify further features that people would expect together with such privacy-awareness features. First of all, one negative aspect mentioned by the participants was that notifications occurred too frequently during the experiment. This issue is due to the experimental design where multiple notifications were simulated in a short time frame. In a real-life setting, these notifications would occur less frequently since it is also one of the basic design principles that we meet with Styx. Further, the responses clearly showed that people expect features to perform some actions whenever they are informed about harm to their privacy (e.g. blocking access, suggesting an

alternative app, etc.). This is in line with the privacy-as-a-process framework in which prevention, response, and recovery are further important stages of privacy management. In our study, we focused on awareness and transparency only. Positive statements mentioned the comprehensibility of the privacy information and its clear and concise visual representation.

5.1. *Implications*

With our research results, we support the adoption of new approaches to privacy risk communication. Particularly, we suggest more directly communicating the potential consequences of using certain services to users, instead of only informing them about potential information flows. Making privacy risks and potential consequences of behavior more explicit will help individuals in making more informed choices. Potential actors to adopt our user interface designs are designers and developers of any kind of privacy-affecting technologies, especially those developing privacy-awareness features. In the context of smartphones, platform providers such as Google or Apple could add features like Styx for monitoring privacy sensitive information flows and providing their users more intuitive and useful privacy information about their apps. Since access to sensitive resources are managed by the smartphone platforms already, such additional features would not require significant changes to the operating systems. Alternatively, privacy monitoring tools such as TaintDroid (Enck et al., 2010) could be extended by the pattern-based privacy monitoring features of Styx. As already indicated in Section 3.1.3, TaintDroid or similar systems could be used as the information-flow monitoring component of Styx and the pattern-matching and notification features could be build on top of that. However, such information-flow monitoring systems require a modification of the smartphone platform and therefore cannot be implemented and installed as regular apps. This would have a significant negative impact on the adoption of such systems.

The impact-level privacy risk communication as proposed in this work could further be adopted by privacy protection and control mechanisms. Instead of giving users fine-grained control over information flows on a data-access level, it could be more effective and intuitive to provide them with control on an impact level. The PIBP approach for example could serve as a basis for a more useful, intuitive, and effective privacy management. A suggestion for privacy researchers is to investigate how the second-order privacy risk perspectice can be further developed or extended. Still, there is a big research challenge in conceptualizing potential consequences regarding privacy-affecting behavior and in finding approaches to communicate the potential consequences to users. Our research results provide a first insight into how to design such awareness features and their effectiveness.

5.2. *Limitations*

There are some limitations of our research results. First, we investigated the effects of the second-order privacy risk communication approach only in a limited context, with a partial implementation of Styx, with a small number of apps, a small and simple set of potential consequences, and a relatively small population. The small sample size has an impact on the statistical power of the calculations, i.e. some existing effects might not have been detected in the data. The small sample size also did not allow an investigation of potential effects of moderating variables such as gender or age or to validate structural models in which the interdependencies between different variables are considered. To gain deeper insight into the effectiveness of our approach, a larger-scale field experiment with a full implementation of Styx could be conducted, which will also help to understand the long-term effects on user perceptions and behavior. Another limitation of our work is that we did not implement and evaluate a full implementation of Styx as presented in Section 3.1.3. Therefore, we cannot provide information about required computational power and the resource overhead that such a system would cause. Yet, successful implementations of privacy monitoring features (e.g. TaintDroid) provide evidence that such features can be provided with reasonable overhead.

Our research was about investigating on how privacy risk communication can be improved in the context of smartphone apps. Anyhow, the results can potentially be applied to other privacy-affecting services, systems or technologies that automatically access and process personal data and sensitive resources to a similar extent (e.g. “smart home”, wearable information technology, in-car information technology). This requires further empirical investigations, though.

6. Conclusion

In this paper, we introduced Styx as an approach to provide smartphone users with more intuitive and semantics-oriented privacy information about their apps. Our aim was to increase the comprehensibility of privacy risks, and at the same time increase trust and reduce concern towards smartphone apps. With Styx we contribute to the knowledge base of human factors in privacy by developing and testing a new method to model and communicate the privacy-related impacts of smartphone usage. We also contribute to the design knowledge for more intuitive privacy-awareness mechanisms.

Our data shows that Styx scores very well regarding these aspects. Compared to traditional privacy risk-communication approaches, the Styx privacy user interfaces were more comprehensible and participants also appreciated it being an innovative approach for privacy warnings. Our data further revealed that Styx is easy to understand and use. At the same time, the data clearly shows that such an privacy-awareness system should only be deployed in combination with privacy control mechanisms. This is in-line with the Privacy Space Framework, where the phases of prevention, response, and recovery immediately follow the phases of awareness and detection. Our results further show that more effective transparency mechanisms can increase user trust towards the smartphone and significantly reduce privacy concerns when interacting with the device. We believe that smartphone vendors could use such trust mechanisms as competitive advantage in future when even more operating systems and apps will be available in the smartphone ecosystem.

We also want to note that run-time privacy warnings should not be the ultimate way to communicate privacy

information to the user. Privacy risk communication should happen as early as possible (e.g. in the app discovery phase). However, the basic principle behind the privacy-impacting behavior approach is monitoring application behavior during run-time and thus, run-time notifications are a suitable method to detect and communicate privacy-impacting application behavior. We further propose that privacy information gathered about apps should be fed back into the privacy risk communication in the app discovery phase, e.g. they could be integrated into the app markets. This will further help users in making safer decisions at the right time.

Acknowledgments

This research was partially funded by the "Vereinigung von Freunden und Förderern der Johann Wolfgang Goethe-Universität" (600 EUR) and the Faculty of Economics and Business Administration at Goethe University Frankfurt (2000 EUR). We want to thank Tahmine Tozman for her advice concerning the experimental design and the statistical analyses and Ralf Strobel for his support in implementing the Styx prototype. We further thank the anonymous reviewers of the IFIP-SEC 2014 version of this paper for their helpful reviews and the audience at the conference for their useful feedback that helped to produce this improved and extended version.

Appendix. Measurement Instruments

Scales and items (all rated on 6-point Likert scales ranging from 1 = "strongly disagree" to 6 = "strongly agree"	Cronbach's Alpha
Smartphone Privacy Concern	
For me, it is important to know which personal data are accessed by my apps.	. 937
It is important to me to decide myself which personal data can be accessed by an app.	
For me, it is important to know what data my apps collect about me.	
I'm concerned that I don't know what an app knows about me.	
I want my smartphone to inform me about potential privacy risks of app usage.	
It is important for me to know who has access to my personal data in general.	
Trust Smartphone	
This smartphone supports the user in identifying potential misuse of personal data by apps.	.726
I believe that the privacy user interfaces of this smartphone inform the user about potential data misuse by apps.	
I trust this smartphone to protect the user's personal data.	
I believe that this smartphone protects the user's data against harmful apps.	
Comprehensibility	
The privacy information that have been presented on this smartphone were easy to understand.	.823
The privacy information that have been presented on this smartphone were self-explanatory.	
The privacy user interfaces of this smartphone inform the user in an comprehensible way about the privacy risks of an app.	
Ease of Comparing	
With this privacy user interface, it is easy to compare different apps regarding their privacy friendliness.	.916
Differences between apps regarding privacy are easy to identify.	

REFERENCES

Amini S. Analyzing mobile app privacy using Computation and Crowdsourcing. Dissertations. Carnegie Mellon University; 2014.

Bai G, Gu L, Feng T, Guo Y, Chen X. Context-aware usage control for android. In: Security and Privacy in Communication Networks. Springer; 2010. p. 326–43.

Bal G. Revealing privacy-impacting behavior patterns of smartphone applications. In: MoST 2012-Proceedings of the Mobile Security Technologies Workshop 2012, San Francisco, USA; 2012.

Beresford AR, Rice A, Sohan N, Skehin N, Sohan R. MockDroid: trading privacy for application functionality on smartphones. In: In Proceedings of HotMobile 2011, Phoenix, Arizona; 2011.

Böhme R, Köpsell S. Trained to accept? A field Experiment on consent dialogs. In: Proceedings of the 28th International Conference on Human factors in Computing Systems – CHI'10, New York, New York, USA, April 10; 2010. p. 2403.

Bravo-Lillo C, Cranor L, Downs J, Komanduri S, Sleeper M. Improving computer security dialogs. In: Campos P, Graham N, Jorge J, Nunes N, Palanque P, Winckler M, editors. Human-Computer Interaction – INTERACT 2011, Lecture Notes in Computer Science, Vol. 6949; 2011. p. 18–35. Berlin, Heidelberg.

Brunk B. A user-centric privacy space framework. In: Cranor LF, Garfinkel SL, O'Reilly, editors. Security and usability – Designing secure systems that people can use; 2005. p. 401–20.

Bugiel S, Davi L, Dmitrienko A, Fischer T, Sadeghi A-RS. XManDroid: a new Android evolution to mitigate privilege escalation attacks. Center for Advanced Security Research Darmstadt; 2011. Technical Report TR-2011-04.

Carnegie Mellon University. PrivacyGrade: grading the privacy of smartphone apps. 2014. http://privacygrade.org/.

Chia PH, Yamamoto Y, Asokan N. Is this app safe? A large scale study on application permissions and risk signals. In: WWW'12-Proceedings of the 21st International Conference on World Wide Web, Lyon, France; 2012. p. 311–20.

Chittaranjan G, Blom J, Gatica-Perez D. Mining large-scale smartphone data for personality studies. Personal Ubiquitous Comput 2011;17(3):433–50.

Conti M, Nguyen VTN, Crispo B. CRePE: context-related policy enforcement for Android. In: ISC'10-Proceedings of the 13th International Conference on Information Security, October 25–28, 2010, Boca Raton, FL, USA, October 25; 2010. p. 331–45.
Cranor LF. Privacy policies and privacy Preferences. In: Cranor LF, Garfinkel SL, O'Reilly, editors. Security and usability – Designing secure systems that people can use; 2005. p. 447–71.
Eagle N, Pentland AS, Lazer D. Inferring friendship network structure by using mobile phone data. Proc Natl Acad Sci 2009;106(36):15274–8.
Egele M, Kruegel C, Kirda E, Vigna G. PiOS: detecting privacy leaks in iOS applications. In: Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS), 6–9 February 2011, San Diego, California; 2011.
Egelman S, Tsai J, Cranor LF, Acquisti A. Timing is everything?: The effects of timing and placement of online privacy indicators. In: Proceedings of the 27th International Conference on Human Factors in Computing Systems (CHI'09), New York, New York, USA, April 4; 2009. p. 319.
Enck W. Defending users against smartphone apps: techniques and future directions. In: Seventh International Conference on Information Systems Security (ICISS 2011), Kolkata, India; 2011.
Enck W, Ongtang M, McDaniel P. On lightweight Mobile phone application certification. In: Proceedings of the 16th ACM conference on Computer and communications security – CCS'09, New York, New York, USA, November 9; 2009. p. 235.
Enck W, Gilbert P, Chun B, Cox LP, Jung J, McDaniel P, et al. TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones. In: Proceedings of USENIX Symposium on Operating Systems Design and Implementation (OSDI), Vancouver, BC; 2010.
European Parliament & Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 1995. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046.
Fang Z, Han W, Li Y. Permission based android Security: Issues and countermeasures. Comput Secur 2014;(43):205–18.
Federal Trade Commission. Android flashlight app developer settles FTC charges it deceived consumers|Federal Trade Commission. 2013. http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.
Federal Trade Commission. Path social networking app settles FTC charges it deceived consumers and improperly collected personal information from users' Mobile Address Books|Federal Trade Commission. 2013. http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived.
Felt AP, Chin E, Hanna S, Song D, Wagner D. Android permissions demystified. In: Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS'11), New York, New York, USA, October 17; 2011. p. 627.
Frank M, Biedert R, Ma E, Martinovic I, Song D. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf. Forensics Secur 2013;8(1):136–48.
Friedman B, Howe DC, Felten E. Informed consent in the Mozilla Browser: implementing value-sensitive design. In: Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Big Island, Hawaii; 2002.
Fu B, Lin J, Li L, Faloutsos C, Hong J, Sadeh N. Why people hate your app: making sense of user feedback in a Mobile app store. In: Proceedings of the 19th ACM SIGKDD International conference on knowledge discovery and data mining – KDD'13, New York, New York, USA, August 11; 2013. p. 1276.
Fuchs AP, Chaudhuri A. SCanDroid: Automated security certification of Android applications. Manuscript, Univ. of Maryland; 2009. http://www.cs.umd.edu/avik/projects/scandroidascaa.
Gilbert P, Chun B-G, Cox LP, Jung J. Vision: automated security validation of mobile apps at app markets. In: Proceedings of the second International Workshop on Mobile cloud computing and services – MCS'11, New York, New York, USA, June 28; 2011. p. 21.
Goecks J, Mynatt ED. Social approaches to end-user privacy management. In: Cranor LF, Garfinkel SL, O'Reilly, editors. Security and usability – Designing secure systems that people can use; 2005. p. 523–45.
Hornyack P, Han S, Jung J, Schechter S, Wetherall D. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In: CCS'11-Proceedings of the 18th ACM conference on Computer and communications security, New York, New York, USA, October 17; 2011. p. 639.
ISO. ISO/IEC29100: Information technology|Security Techniques | privacy framework. No. ISO/IEC29100. 2011., http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.
Kelley PG, Bresee J, Cranor LF, Reeder RW. A 'Nutrition label' for privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09), New York, New York, USA, July 15; 2009.
Kelley PG, Consolvo S, Cranor LF, Jung J, Sadeh N, Wetherall D. A conundrum of permissions: installing applications on an Android smartphone. In: Proceedings of Workshop on Usable Security (USEC 2012), Kralendijk, Bonaire; 2012. p. 1–12.
Kwapisz JR, Weiss GM, Moore SA. Cell phone-based biometric identification. In: Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2010), Washington, DC; 2010. p. 1–7.
Laughery KR, Vaubel KP, Young SL, Brelsford JW, Rowe AL. Explicitness of consequence information in warnings. Saf Sci 1993;16(5–6):597–613.
Laugwitz B, Schrepp M, Held T. Konstruktion eines Fragebogens zur Messung der User Experience von Softwareprodukten. In: Heinecke AM, Paul H, editors. Mensch & Computer 2006: Mensch und Computer im Strukturwandel. München: Oldenbourg Verlag; 2006. p. 125–34.
Lederer S, Hong J, Dey A, Landay J. Personal privacy through understanding and action: five pitfalls for designers. Personal Ubiquitous Comput 2004;8(6):440–54.
Lin J, Amini S, Hong J, Sadeh N, Lindqvist J, Zhang J. Expectation and purpose: understanding users' Mental models of Mobile app privacy through Crowdsourcing. In: Proceedings of the 14th ACM International Conference on Ubiquitous Computing – Ubicomp 2012, Pittsburgh, Pennsylvania, USA; 2012. p. 501–10.
Lin J, Liu B, Sadeh N, Hong JI. Modeling users' Mobile app privacy preferences: restoring usability in a sea of permission settings. In: Symposium on Usable Privacy and Security (SOUPS 2014), Menlo Park, CA; 2014.
Meng Y, Wong D, Schlegel R, Kwok L. Touch gestures based biometric authentication scheme for touchscreen mobile phones. In: Kutyłowski M, Yung M, editors. Information Security and Cryptology. Heidelberg: Springer Berlin; 2013.
Milne GRG, Culnan MMJ. Strategies for reducing online privacy risks: why consumers read (or Don't read) online privacy notices. J Interact Mark 2004;18(3):15–29.
Min J, Wiese J, Hong JI, Zimmerman J. Mining smartphone data to classify life-facets of social relationships. In: Conference on Computer Supported Cooperative Work and Social Computing (CSCW 2013), San Antonio, Texas, USA; 2013.
Nauman M, Khan S, Zhang X. Apex: Extending Android permission model and enforcement with user-defined

runtime constraints. In: ASIACCS'10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ASIACCS'10; 2010. p. 328–32.
OECD. Guidelines on the protection of privacy and transborder flows of personal data. 1980. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
Owusu E, Han J, Das S, Perrig A, Zhang J. ACCessory: password inference using accelerometers on smartphones. In: Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications. New York, New York, USA: HotMobile'12; 2012. p. 1. February 28.
Phithakkitnukoon S, Horanont T, Di Lorenzo G, Shibasaki R, Ratti C. Activity-aware Map: identifying human daily activity pattern using Mobile phone data. In: Salah AA, Gevers T, Sebe N, Vinciarelli A, editors. Human Behavior Understanding, Lecture Notes in Computer Science, Lecture Notes in Computer Science, Vol. 6219. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010. p. 14–25.
Sasse M, Flechais I. Usable security: why do we need it? How do we get it? In: Cranor LF, Garfinkel SL, O'Reilly, editors. Security and usability – Designing secure systems that people can Use; 2005. p. 13–30.
Schneier B. Secrets & lies: digital security in a networked world. 1st ed. New York, NY, USA: John Wiley & Sons, Inc; 2000.
Shi E, Niu Y, Jakobsson M, Chow R. Implicit authentication through learning user behavior. In: Burmester M, Tsudik G, Magliveras S, Ilić I, editors. Information Security SE – 9, Lecture Notes in Computer Science, Vol. 6531. Springer Berlin Heidelberg; 2011a. p. 99–113.
Shi W, Yang J, Jiang Y. Senguard: passive user identification on smartphones using multiple sensors. In: Proceedings of the 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Wuhan, China; 2011. p. 141–8.
Slovic P. Perception of risk. Science 1987;236(4799):280–5.
Slovic P. In: Slovic P, editor. The perception of risk. 1st ed. Earthscan Publications; 2000.
Tan J, Nguyen K, Theodorides M, Negrón-Arroyo H, Thompson C, Egelman S, et al. The effect of developer-specified explanations for permission requests on smartphone user behavior. In: Proceedings of the 32nd annual ACM conference on Human factors in computing systems – CHI'14, New York, New York, USA, April 26; 2014. p. 91–100.
Tey CM, Gupta P, GAO D. I can Be you: questioning the use of keystroke dynamics as biometrics. In: The 20th Annual Network & Distributed System Security Symposium (NDSS 2013), San Diego, CA, USA; 2013.
Thampi A. Path uploads your entire iPhone address book to its servers. 2012. http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html.
Thompson C, Johnson M, Egelman S, Wagner D, King J. When it's better to ask forgiveness than get permission. In: Proceedings of the Ninth Symposium on Usable Privacy and Security (SOUPS'13), Newcastle, UK; 2013.
TÜV Rheinland. Die TÜV Rheinland Datenschutzprüfung 'Check Your App. 2014. https://www.checkyourapp.de/.
United States Congress. An Act to amend title 5, United States Code, by adding a section 552a, to safeguard individual privacy from the misuse of Federal records, to provide that individuals be granted access to records concerning them which are maintained by Federal agencies. 1974. http://www.justice.gov/opcl/privacy-act-1974. http://www.justice.gov/opcl/privacy-act-1974.
U.S. Department of Health Education and Welfare. Secretary's Advisory Committee on Automated personal data systems, records, computers, and the rights of citizens. HEW Report. 1973., https://www.epic.org/privacy/hew1973report/.
Weiss GM, Lockhart JW. Identifying user traits by mining smart phone accelerometer data. In: Proceedings of the Fifth International Workshop on Knowledge Discovery from Sensor Data (SensorKDD'11), New York, New York, USA; 2011. p. 61–9.
Zheng N, Bai K, Huang H, Wang H. You are how you touch: user verification on smartphones via tapping behaviors. In: IEEE 22nd International Conference on Network Protocols (ICNP 2014), Raleigh, NC, October; 2014. p. 221–32.
Zhou Y, Zhang X, Jiang X, Freeh VW. Taming information-stealing smartphone applications (On Android). In: Trust and Trustworthy Computing. Springer; 2011. p. 93–107.

Gökhan Bal is a Ph.D. candidate and Research Assistant at the Deutsche Telekom Chair of Mobile Business and Multilateral Security, Department of Business Informatics, Goethe University Frankfurt. Gökhan has a degree in Computer Science (M.Sc.) from Goethe University Frankfurt, while he completed his final thesis at the Fraunhofer Institute for Secure Information Technology in Darmstadt. His main research interests are in behavioral privacy and security research and the focus of his Ph.D. research is on improving privacy-risk communication in smartphone app ecosystems.

Kai Rannenberg holds the Deutsche Telekom Chair of Mobile Business & Multilateral Security at Goethe University Frankfurt since 2002. Before he was working with the System Security Group at Microsoft Research Cambridge on „Personal Security Devices & Privacy Technologies". Since 1991 Kai is active in ISO/IEC standardization in JTC 1/SC 27/WG 3 "Security evaluation criteria". In 2007, he became Convenor of SC 27/WG 5 "Identity management and privacy technologies". 2004 till 2013 Kai served as the academic expert in the Management Board of the European Network and Information Security Agency, and is now a member of ENISA's Permanent Stakeholder Group.

Jason Hong is an associate professor in the Human Computer Interaction Institute, part of the School of Computer Science at Carnegie Mellon University. He works in the areas of ubiquitous computing and usable privacy and security, and his research has been featured in the New York Times, MIT Tech Review, CBS Morning Show, CNN, Slate, and more. Jason received his PhD from Berkeley and his undergraduate degrees from Georgia Institute of Technology. Jason has participated on DARPA's Computer Science Study Panel (CS2P), is an Alfred P. Sloan Research Fellow, a Kavli Fellow, and a PopTech Science fellow.