Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones

Gökhan Bal, Kai Rannenberg, Jason Hong

▶ **To cite this version:**

Gökhan Bal, Kai Rannenberg, Jason Hong. Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones. 29th IFIP International Information Security Conference (SEC), Jun 2014, Marrakech, Morocco. pp.113-126, 10.1007/978-3-642-55415-5_10 . hal-01370359

HAL Id: hal-01370359

https://inria.hal.science/hal-01370359

Submitted on 22 Sep 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Styx: Design and Evaluation of a New Privacy Risk Communication Method for Smartphones

Gökhan Bal[1], Kai Rannenberg[1], and Jason Hong[2]

[1] Goethe University Frankfurt, Germany
{goekhan.bal,kai.rannenberg}@m-chair.de
[2] Carnegie Mellon University, Pittsburgh, PA, USA
jhong@cs.cmu.edu

Abstract. Modern smartphone platforms are highly privacy-affecting but not effective in properly communicating their privacy impacts to its users. Particularly, *actual* data-access behavior of apps is not considered in current privacy risk communication approaches. We argue that factors such as frequency of access to sensitive information is significantly affecting the privacy-invasiveness of applications. We introduce Styx, a novel privacy risk communication system that provides the user with more meaningful privacy information based on the actual behavior of apps. In a proof-of-concept study we evaluate the effectiveness of Styx. Our results show that more meaningful privacy warnings can increase user trust into smartphone platforms and also reduce privacy concerns.

1 Introduction

Technological innovations in the area of consumer electronics developed by far faster than our ability to assess their implications on our social lives. Information privacy is one of the facets in consumer life that experiences the most substantial change. For the sake of innovation and utility, consumers have unconcernedly (or unknowingly) given away the control over their personal data. Most designers of privacy-affecting systems[3] don't define the protection of consumer privacy as a primary goal and thus, privacy-awareness or privacy-protection mechanisms usually are not a prominent feature in most technologies.

Modern smartphone platforms have unique properties that make them highly privacy-affecting, i.e. 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, and they provide those applications with access to a multiplicity of sensitive resources such as the GPS module, the user's contacts, call log, or browsing history. The dynamics and the quantity of sensitive information flows on smartphone platforms require sophisticated approaches for giving back the consumers the control over their data. According to the *Privacy Space Framework*, information privacy protection is a process that starts with *awareness* and *detection*

[3] Based on Lederer et al. (2005) [26], we define privacy-affecting systems as any interactive system whose use has personal privacy implications.

of privacy issues [5]. Consequently, solutions have also to improve these two mechanisms.

The use of personal data by third-party applications affects the users' privacy in varying extent. Factors influencing the extent are e.g. the type of data that is processed, the frequency of access, or the destination of sensitive information flows. Ideally, privacy-awareness solutions reflect those dependencies in their underlying mechanisms. In practice, the users are too often not even aware that sensitive resources have been accessed by applications. Privacy-related notices are in most cases not successful in informing the users appropriately about the actual privacy risks of the services. One major explanation for this is that in most cases the underlying model for privacy risks is limited to access-control information such as granting an application access to some resources. Other commonly known explanations are the extensive length of privacy policies, the frequent use of technical or legal terminology, or the inappropriate timing of privacy notices. We argue that privacy-awareness measures should move from *access-control level* to *privacy-impact level*. In other words, privacy-awareness systems should not (solely) inform users about single information flows. Instead, the mechanisms should reason about multiple information flows that happen over time and look at the actual privacy-impacting behavior of an app. The (user-facing) outcome of those mechanisms should be concrete privacy-impact information that relate to the individual behavior of apps. In this paper we propose *Styx*[4], which is such a privacy-awareness system for smartphone platforms. We use *privacy-impacting behavioral patterns (PIBP)* [2] as the conceptual basis for our system. PIBPs are a model for privacy impacts that bridge the gap between multiple information flows and their impact on user privacy.

The contributions of this paper are as follows: 1. we present the design principles and a proof-of-concept implementation of Styx, a novel privacy-awareness system for the Android smartphone platform, 2. we present results from an experimental evaluation of Styx to demonstrate its utility, focusing on human factors. We contribute to the knowledge base of information privacy technology design, especially regarding privacy risk communication methods.

The paper is structured as follows. Section 2 summarizes and integrates relevant concepts and theories from the knowledge base. Section 3 provides some key definitions and subsequently presents design principles for Styx that we have identified from information privacy literature. Section 4 then introduces and elaborates in more detail the conceptual basis for Styx, namely the privacy-impacting behavioral patterns. Following on that, Section 5 proposes an architectural design for Styx. The components of Styx that we have developed as proof-of-concept are introduced in Section 6. Details about the evaluation are presented in Section 7. We conclude this paper with a discussion on the results (Section 8).

[4] Inspired by the river "Styx" from Greek mythology, which formed a boundary between the world of the living and the Underworld. We use this as a metaphor for sensitive information flows between the user's "realm" and the hidden, "dark side" of the smartphone device.

2 Related Work

This section provides an overview of the relevant literature in smartphone privacy research, which will help to understand how our research on Styx was informed by the body of knowledge. Due to space restrictions, we do not describe single research results in detail.

The Nature of Privacy Risks of Smartphone Usage. On the very basic level, the privacy risks of smartphone app usage are about the leakage of sensitive information from the user's device [31]. With *TaintDroid*, Enck et al. [14] revealed that privacy-breach incidents are not rare, many apps are sending sensitive data to their servers without informing the user. On a more semantic level, privacy risks result due to the long-term usage of apps. Data mining-based approaches demonstrate the potentials of inferring user identity-related information based on data that is available on the devices or collected by apps over time. Kwapisz et al. show how collected accelerometer data can be used to uniquely identify the user [24]. Weiss et al. [33] show how the same source of information can even be used to identify user traits such as sex, height, and weight of the user. Similar results can be found in [8], [28], [11], [30], and [19].

Smartphone Users' Perception of Privacy Risks. Privacy indicators or warnings should both motivate users to respond, and help them understand the risk of the used services [4]. Besides privacy policies that exist for some apps, Android's permission request screen, which shows up each time the user wants to install an application, can be regarded as Android's main indicator for the potential impacts on user privacy. However, researchers have demonstrated that permission screens are not effective privacy indicators. Often users don't notice this screen or they have difficulties in understanding the risk signals [23]. Chia et al. showed that none of the existing risk signals in the smartphone app ecosystem are effective as indicators for the privacy risks [7].

Alternative Privacy Indicators. Kelley et al. [22] used the nutrition-label approach to represent privacy information taken from privacy policies of online services. Another approach to improve privacy information on the Android platform is to use attribution mechanisms which is a method 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 [32]. The approach taken by Lin et al. [27] 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". Egelman et al. (2009) could show that the timing had a significant impact on the behavior of users in the context of online shopping [13]. Alternative designs for privacy indicators have an effect on the

user's behavior, but yet so far there is no approach that considers the multiplicity of potential sensitive information flows and their very dynamic nature on smartphone platforms when modeling privacy risks.

Technologies for Enhanced Privacy Control. Many tools have been developed in recent years that aim to analyze or enhance the privacy level of smartphone platforms. One category of such tools are *information flow analyzers* that analyze smartphone applications regarding potential privacy breaches before they are installed on users' devices. Some of the more prominent examples are *Kirin* [15], *AppInspector* [18], *Stowaway* [16], *SCanDroid* [17], *PiOS* [12], *TaintDroid* [14], and *XManDroid* [6]. Except for Kirin, the mentioned approaches have a limited model for the actual privacy risk.

Enhanced Information Flow Control. Some privacy tools provide the users a more fine-grained or context-sensitive control over their data. Examples are *TISSA* [34], *Apex* [29], *CRePE* [9], and *ConUCON* [1]. Another form of enhanced information flow control for smartphone users is replacing real data with mocked data when apps want to access sensitive resources [21] and [3]. The concepts listed here are useful approaches for the prevention and response phases of information privacy control. Our focus is on the awareness and detection phases of the privacy space framework.

3 Design Principles and Guidelines

Existing literature on privacy theories and tools provide valuable guidelines for the design of privacy mechanisms. Our requirements analysis for Styx resulted in a set of principles and guidelines that we present in the following. Also, we introduce some key terms that will help the reader in integrating our contributions into the bigger picture of privacy research.

3.1 Working Definitions and Relevant Concepts

We see information privacy rather as a process as defined in the Privacy Space Framework [5]. The proposed phases of information privacy management are *awareness, detection, prevention, response*, and *recovery*. With Styx we target the phases awareness and detection. Another important concept that informed our research was the concept of *Exoinformation*. Generally speaking, exoinformation is *new* information that is gathered by putting together and analyzing *available* information [5]. The PIBP approach introduced in Section 4 can be regarded as a specific implementation of the exoinformation concept.

3.2 Design Principles

From the usable privacy literature we have identified a set of design guidelines that inform the design of Styx:

- avoid the use of privacy jargons (DP1),
- communicate the existence of a threat (DP2) [26],
- filter information and alert users only to potentially important or new concerns and threats (DP3),
- minimal distraction (DP4),
- do not obscure actual and potential information flow (DP5) [20],
- provide educational opportunities to users (DP6) [10],
- provide meaningful summaries of privacy information (DP7),
- consider exoinformation (DP8).

4 Privacy-impacting Behavioral Patterns

As the conceptual basis for Styx we use privacy-impacting behavioral patterns [2]. The basic idea behind the PIBP concept draws on the concept of exoinformation. The most common approach for privacy notices is to inform users about single, potentially privacy-impacting, information flows. In this case, privacy risks are modeled as a single data leakage[5]. The assumption here is that consumers are able to map that specific information flow instance to the impact it will have on their privacy. The 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, thus it is a function of time. A one-time access to the resource will not exploit the full potentials of knowledge extraction. Rather, the more often an application accesses the user's current location, the more information can be extracted about the user. An app that accesses the user's location every 30 minutes 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 geo-location every 30 minutes or more often". One could think of much more complex examples where for example different sensitive resources are combined.

5 Styx

In this section we present the conceptual architecture of Styx, a PIBP-implementing, privacy-awareness system for the Android platform. We will further present a proof-of-concept implementation of Styx and demonstrate how the requirements of Section 3 are met.

5.1 Styx Architecture

Figure 1 shows the proposed components for a PIBP-implementing system. These components are introduced in the following.

Styx Monitoring. This component is responsible for dynamically monitoring sensitive information flows between the device and applications. TaintDroid [14] could be used as the implementation of this component.

[5] Simple example: "Application A wants to access your location"

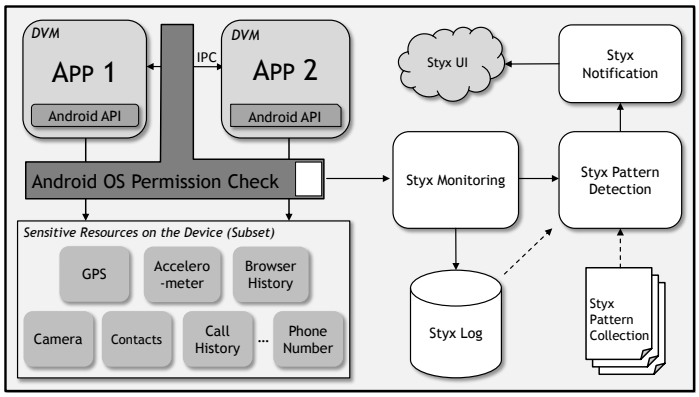

Fig. 1. Conceptual architecture of Styx

Styx Log. Information about information flows will be stored here. The monitoring component is responsible for creating new log entries.

Styx Pattern Collection. Since we model privacy impacts as behavioral patterns of apps, Styx must have access to a set of such privacy-impacting behavioral patterns in order to match application behavior with privacy impacts. Pre-defined patterns are stored in the pattern collection database.

Styx Pattern Detection. The actual matching between observed app behavior and PIBPs is performed by the Styx Pattern Detection engine. This component is triggered by the monitoring component after a new entry has been stored in the log. The pattern detection mechanisms 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 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.

6 Proof-of-Concept

We have implemented a proof-of-concept of Styx for the purpose of evaluating its effectiveness. As stated in the beginning of this paper, Styx targets the awareness and detection phases of the information privacy process. 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 the proof-of-concept. The Styx UI is composed of six different screens that represent different types

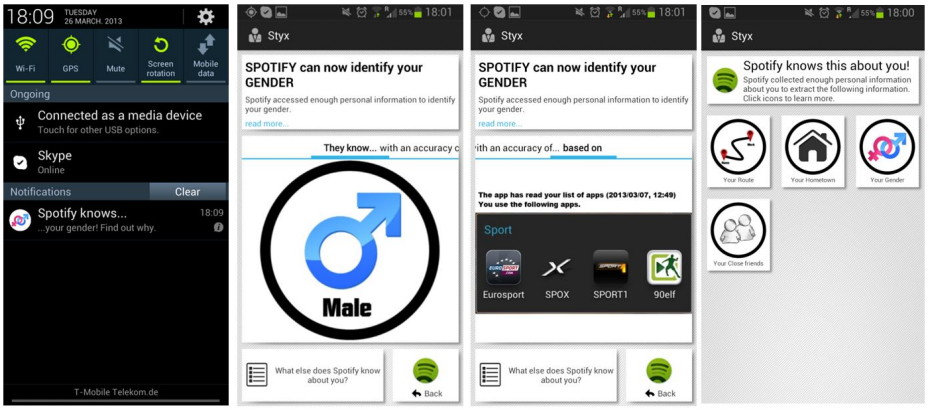

Fig. 2. Styx screenshots

and levels of privacy information. The respective purposes of the screens are described in the following.

1. **Styx Notification.** The first screen that the user sees is the notification and the respective entry in the notification menu (a. in Figure 2).
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 identity-related inference the currently used app could make about the user (in the simple example it's the user's gender; b. in Figure 2).
3. **Styx Rating.** The purpose is to help users understand whether the applications 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?").
4. **Styx Basis Screen.** We want to make the underlying mechanisms of Styx transparent to the user by also informing him about the privacy-impacting behavior of the app (i.e., which resources did it access in what manner?). At the same time, this is an educational part of Styx (DP6). The users will be able to better understand the relation between concrete privacy impacts and access to sensitive information (c. in Figure 2). In the example, 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 user more detailed information when he clicks on the "Learn more..." part of the inference screen.
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 has already inferred in the past (DP7). 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 (d. in Figure 2).

6.1 Meeting the Requirements

Styx is an implementation of the PIBP concept. As such, actual and potential information flows are considered when assessing the privacy impacts of app behavior (DP5). Furthermore, the PIBP concept can be regarded as an instantiation of the exoinformation concept, thus exoinformation are considered by design (DP8). The ultimate goal of Styx is communicating the existence of privacy threats. It does so by analyzing what potential identity-related inferences an app can make about the user, based on what is has accessed so far and then inform the user about these specific threats (DP2). Another advantage of the PIBP approach is that it does not notify the user on information-flow level. Rather, multiple information flows are observed, aggregated and analyzed (DP3). Only when a certain privacy-impacting behavior has been detected, the user gets notified, so the number of distractions from the user's primary task is reduced (DP4). In the Styx UI, we avoid technical terms (DP1), educational opportunities are provided by the Styx Basis Screen and the Styx Detailed Information Screen (DP6). A privacy summary of an app is provided by the Styx Dashboard (DP7).

7 User Study

We evaluated the Styx proof-of-concept in a user study in spring of 2013. We set up an in-lab experiment at Carnegie Mellon University. We recruited participants through the *CBDR Participant Portal*[6] of the university. We invited people to "A User Study about Smartphone apps". Participants were compensated with a $10 gift card for their time.

7.1 Participants

In total, 77 participants registered for the user study. 50 of those showed up during the two-week experiment phase. 18 of the participants were female (36%), 32 were male (64%). 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. The participants had installed M=25.54 apps (SD=25.32) on their devices and used M=9.12 apps regularly (at least once a week; SD=7.13).

[6] The CBDR Participant portal is an online system that help researchers in organizing their user studies.

7.2 Experimental Design

The experiments have been conducted in the Human-Computer Interaction Institute at Carnegie Mellon University. We invited one participant at a time to do the experiment, which took approximately one hour per participant. We used a *between-subjects* design for the experiment, since we wanted to test Styx against an alternative approach that is based on current risk communication schemes. Before starting the experiment, participants were randomly assigned to one of the two conditions. We handed the participants a smartphone[7] on which the respective tool was running in the background. After introducing them 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. The tasks were mainly about starting specific apps[8] and using some of their core features. In pre-defined points in time, the device showed notifications in the notification bar and played a sound while showing up. Participants in the *experimental condition* have been shown the Styx privacy user interfaces, participants in the *control condition* have been faced with an alternative run-time privacy UI that will provide the user with a chronologically ordered information flow history. By introducing a run-time component to the control condition, we made the comparison fair[9]. The participants were free to examine the notifications. Only in the case of the weather and the running app we explicitly instructed them to examine the notification and the respective user interfaces.

7.3 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.

Questionnaire The main goal of the user study was evaluating the new privacy risk communication method regarding *comprehension* of the communicated privacy information. However, it is also important to look at the impact of the new approach on user trust and privacy concern. We believe that effective transparency mechanisms can increase *trust* into the smartphone platform and reduce privacy *concern*. Therefore, we added these two variables as dependent variables to the questionnaire. We proposed Styx as an innovative approach to communicate privacy risks of smartphone apps. To assess novelty, we used the respective scale from the *User Experience Questionnaire (UEQ)* (Laugwitz et al. [25]). 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". Example items: "The privacy information was self-explanatory" (comprehension), "I trust this smartphone to protect

[7] Samsung Galaxy S3 LTE.

[8] We used five types of apps during the experiment: flashlight, weather, dice, running tracker, and a kids memory game

[9] Otherwise, the pure existence of privacy information in the experimental group would lead to biased data.

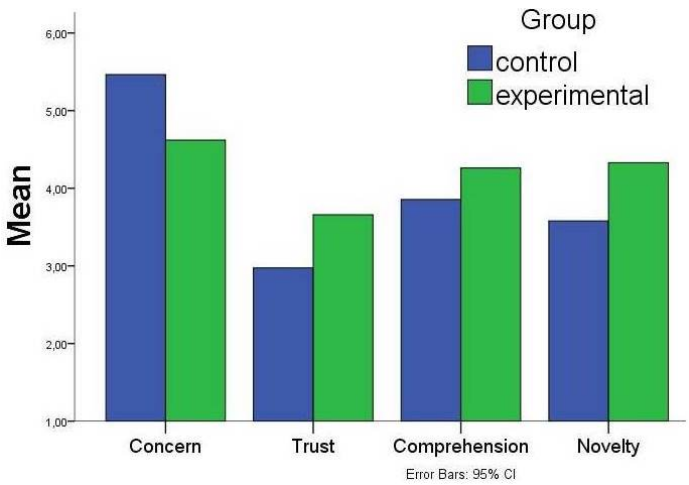

Fig. 3. Mean values of the questionnaire scales

the user's data against harmful apps" (trust), "I'm concerned that the apps have accessed personal data without informing me" (concern), "The presented privacy user interfaces were innovative" (novelty).

Qualitative Data As part of the evaluation, we also asked the participants in the questionnaire what they particularly liked and did not like about the new privacy user interface. Participants could enter up to five aspects per question.

7.4 Data Analysis

Questionnaire Figure 3 shows the mean scores for the concern, trust, comprehension, and novelty scales for the two conditions. The experimental group scores better in all four scales, while the differences in the concern (M_{exp}=4.62, M_{ctrl}=5.46) and novelty (M_{exp}=4.33, M_{ctrl}=3.58) scales are statistically significant ($p<.05$). There are strong tendencies in the mean values of the trust (M_{exp}=3.66, M_{ctrl}=2.97) and comprehension (M_{exp}=4.26, M_{ctrl}=3.86) scales.

Qualitative Data When looking at the responses to the question "what did you *not* like about the privacy user interface?", 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")[10]. Three responses were about the

[10] The issue with the notifications is due to the experimental design where multiple notifications were simulated in a short time frame. In a real setting, these notifications would occur less frequently.

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 qualitative 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.

8 Discussion and Conclusion

Styx is our proposed approach to provide smartphone users with more intuitive and semantic 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 the smartphone. 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. The qualitative 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 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 PIBP 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 gathered privacy information 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. 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.

Acknowledgments. This research was partially funded by the *Vereinigung von Freunden und Förderern der Johann Wolfgang Goethe-Universität* and the Faculty of Economics and Business Administration at Goethe University Frankfurt. We further thank Tahmine Tozman for her advice concerning the experimental design and Ralf Strobel for his support in implementing the prototype.

References

1. Bai, G., Gu, L., Feng, T., Guo, Y., Chen, X.: Context-Aware Usage Control for Android. In: Security and Privacy in Communication Networks, pp. 326–343. Springer (2010)
2. Bal, G.: Revealing Privacy-Impacting Behavior Patterns of Smartphone Applications (Short Paper). In: MoST 2012 - Proceedings of the Mobile Security Technologies Workshop 2012. San Francisco, USA (2012), http://mostconf.org/2012/papers/15.pdf
3. Beresford, A.R., Rice, A., Sohan, N., Skehin, N., Sohan, R.: MockDroid: trading privacy for application functionality on smartphones. In: In Proceedings of HotMobile 2011. ACM (2011)
4. 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. (eds.) Human-Computer Interaction INTERACT 2011. Lecture Notes in Computer Science, vol. 6949, pp. 18–35. Springer Berlin Heidelberg, Berlin, Heidelberg (2011), http://www.springerlink.com/content/q551210n08h16970/
5. Brunk, B.: A User-Centric Privacy Space Framework. In: Cranor, L.F., Garfinkel, S.L. (eds.) Security and Usability - Designing Secure Systems that People Can Use, chap. 21, pp. 401–420. O'Reilly (2005)
6. Bugiel, S., Davi, L., Dmitrienko, A., Fischer, T., Sadeghi, A.R.S.: XManDroid: A New Android Evolution to Mitigate Privilege Escalation Attacks. Tech. rep. (2011)
7. Chia, P.H., Yamamoto, Y., Asokan, N.: Is this App Safe ? A Large Scale Study on Application Permissions and Risk Signals. In: Proceedings of WWW 2012. No. November (2012)
8. Chittaranjan, G., Blom, J., Gatica-Perez, D.: Mining large-scale smartphone data for personality studies. Personal and Ubiquitous Computing (Dec 2011), http://www.springerlink.com/index/10.1007/s00779-011-0490-1
9. Conti, M., Nguyen, V.T.N., Crispo, B.: CRePE: Context-related Policy Enforcement for Android. In: ISC'10 Proceedings of the 13th international conference on Information security. pp. 331–345 (Oct 2010)
10. Cranor, L.F., Garfinkel, S.L.: Security and Usability - Designing Secure Systems that People Can Use. O'Reilly (2005)

11. Eagle, N., Pentland, A.S., Lazer, D.: Inferring Social Network Structure using Mobile Phone Data. Tech. Rep. usually 1 (2009)
12. Egele, M., Kruegel, C., Kirda, E.: PiOS : Detecting Privacy Leaks in iOS Applications. In: NDSS 2011 Network and Distributed System Security Symposium Proceedings (2011)
13. Egelman, S., Tsai, J., Cranor, L.F., 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. p. 319. ACM Press, New York, New York, USA (Apr 2009), http://dl.acm.org/citation.cfm?id=1518701.1518752
14. Enck, W., Gilbert, P., Chun, B.g., Cox, L.P., Jung, J., McDaniel, P., Sheth, A.N.: TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In: Proc. of USENIX Symposium on Operating Systems Design and Implementation (OSDI) (2010)
15. 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. p. 235. ACM Press, New York, New York, USA (Nov 2009)
16. Felt, A.P., 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. p. 627. ACM Press, New York, New York, USA (Oct 2011)
17. Fuchs, A.P., Chaudhuri, A.: SCanDroid: Automated Security Certification of Android Applications. Tech. rep., University of Maryland (2009), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.148.2511
18. Gilbert, P., Chun, B.G., Cox, L.P., 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. p. 21. ACM Press, New York, New York, USA (Jun 2011)
19. González, M.C., Hidalgo, C.a., Barabási, A.L.: Understanding individual human mobility patterns. Nature 453(7196), 779–82 (Jun 2008), http://www.ncbi.nlm.nih.gov/pubmed/18528393
20. Hong, J.I.: An Architecture for Privacy-Sensitive Ubiquitous Computing. Ph.D. thesis, UNIVERSITY OF CALIFORNIA (2005)
21. 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. p. 639. ACM Press, New York, New York, USA (Oct 2011)
22. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A "nutrition label" for privacy. In: Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. p. 1. ACM Press, New York, New York, USA (Jul 2009), http://dl.acm.org/citation.cfm?id=1572532.1572538
23. Kelley, P.G., Consolvo, S., Cranor, L.F., Jung, J., Sadeh, N., Wetherall, D.: A Conundrum of Permissions: Installing Applications on an Android Smartphone. In: Proceedings of USEC 2012. pp. 1–12 (2012)
24. Kwapisz, J.R., Weiss, G.M., Moore, S.A.: Cell phone-based biometric identification. In: 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS). pp. 1–7. IEEE (Sep 2010), http://ieeexplore.ieee.org/articleDetails.jsp?arnumber=5634532

25. Laugwitz, B., Held, T., Schrepp, M.: Construction and Evaluation of a User Experience Questionnaire. Tech. rep. (2008)
26. Lederer, S., Dey, A.K., Mankoff, J.: A Conceptual Model and a Metaphor of Everyday Privacy in Ubiquitous Computing Environments. Ubiquitous Computing Computer S (2002), http://www.cs.cmu.edu/~io/publications/old-pubs/privacy-techreport02.pdf
27. 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 (2012)
28. Min, J.k., Wiese, J., Hong, J.I., Zimmerman, J.: Mining Smartphone Data to Classify Life-Facets of Social Relationships. In: Conference on Computer Supported Cooperative Work and Social Computing 2013 (2013)
29. 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. pp. 328–332. ASIACCS '10, ACM Press (2010)
30. 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, A.A., Gevers, T., Sebe, N., Vinciarelli, A. (eds.) Human Behavior Understanding, Lecture Notes in Computer Science, Lecture Notes in Computer Science, vol. 6219, pp. 14–25. Springer Berlin Heidelberg, Berlin, Heidelberg (2010), http://www.springerlink.com/index/10.1007/978-3-642-14715-9
31. Thampi, A.: Path uploads your entire iPhone address book to its servers, http://mclov.in/2012/02/08/path-uploads-your-entire-address-book-to-their-servers.html
32. 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. p. 1 (2013), http://dl.acm.org/citation.cfm?doid=2501604.2501605
33. Weiss, G.M., Lockhart, J.W.: Identifying user traits by mining smart phone accelerometer data. In: Proceedings of the Fifth International Workshop on Knowledge Discovery from Sensor Data - SensorKDD '11. pp. 61–69. ACM Press, New York, New York, USA (2011), http://portal.acm.org/citation.cfm?doid=2003653.2003660
34. Zhou, Y., Zhang, X., Jiang, X., Freeh, V.W.: Taming information-stealing smartphone applications (on Android). In: Proceedings of the 4th international conference on Trust and trustworthy computing (TRUST'11). pp. 93–107 (Jun 2011)