User Control Mechanisms for Privacy Protection Should Go Hand in Hand with Privacy-Consequence Information: The Case of Smartphone Apps

W3C Workshop on Privacy and User–Centric Controls

20–21 November 2014, Berlin, Germany

Dipl.-Inf. Gökhan Bal, Prof. Dr. Kai Rannenberg
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

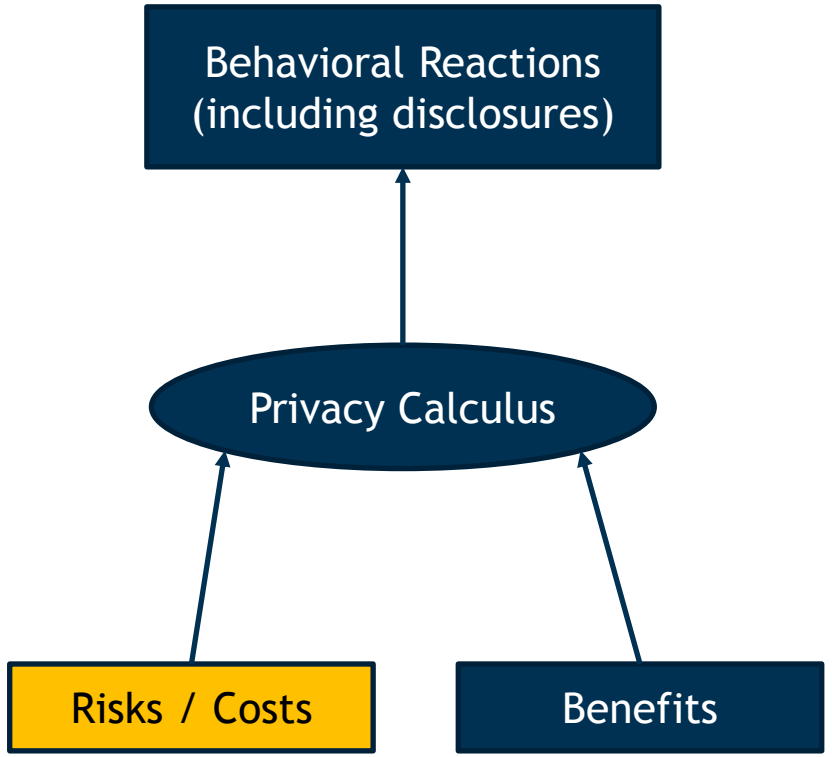
1 MOTIVATION

1. Motivation
Two Perspectives on Privacy Protection

Privacy Protection as a Process (Brunk 2005)

Risk awareness is key!

Decision-making as a calculus of risks and benefits (Culnan and Armstrong 1999)



1. Motivation
Problems

- Benefits are what drive users towards service use.
- Privacy thoughts most often are only a „supporting actor" in users' decision-making.
- More effective privacy-risk communication is needed to help users understand the consequences of behavior.
- **Call: integrate (privacy-)consequence information into user-control mechanisms.**

2 THE CASE OF SMARTPHONE APPS

2 The Case of Smartphone Apps
Privacy Risks of Smartphone App Usage

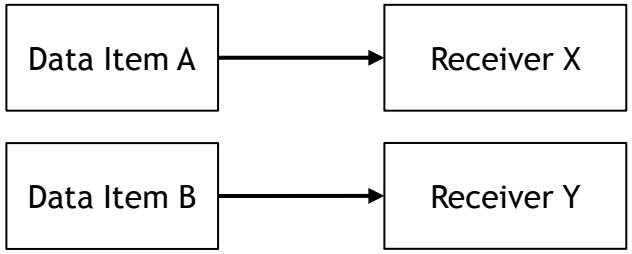
- Apps are useful and provide utility.
- APIs (e.g. geolocation API) as
  - …enabler of utility.
  - …threat to user privacy.
- Negative examples: „Path“ & „Brightest Flashlight“
- Lack of risk transparency and “hidden” information flows lead to a bias in users’ risk perceptions.
- Explicitness regarding consequences can help (Laughery et al. 1993).

2 The Case of Smartphone Apps
Privacy Risks of Smartphone App Usage

First-order privacy risk:

- apps can access a multiplicity of sensitive resources (enabled to provide utility).
- most apps have Internet access.
- information flows often without notice.

→ **risk: leakage of sensitive data[1].**

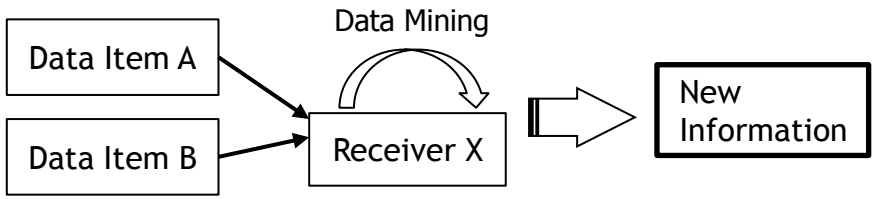


[1]e.g., Egele et al. 2011; Enck et al. 2010

Second-order privacy risk:

- Profiling: aggregated smartphone data can be used to generate meaningful information about the user (predict user traits, personality traits, movement patters)[2]

→ **risk: implicit revelations of private information due to data-aggregation potentials.**

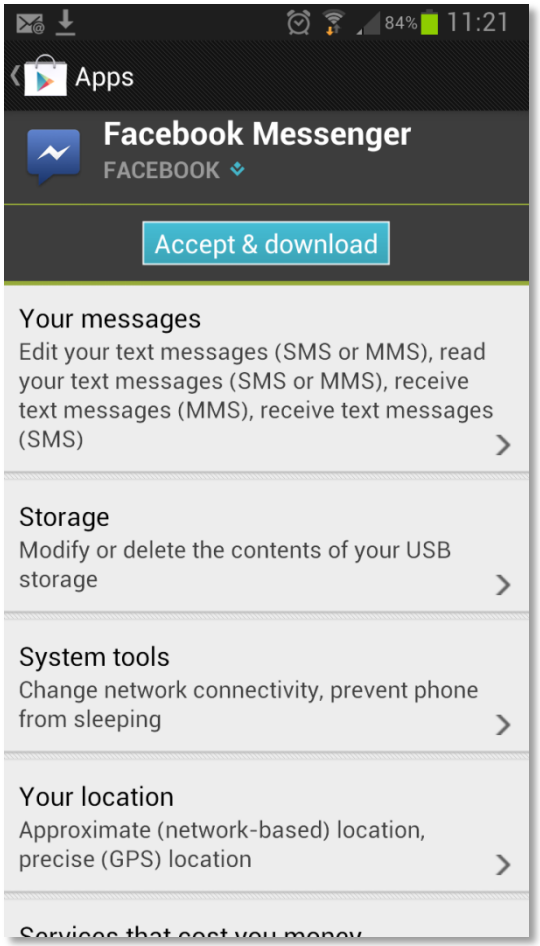


[2]e.g., Kwapisz et al. 2010; Weiss and Lockhart 2011; Chittaranjan et al. 2011; Min et al. 2013; González et al. 2008; Phithakkitnukoon et al. 2010.

2 The Case of Smartphone Apps
Current Privacy-Risk Communication

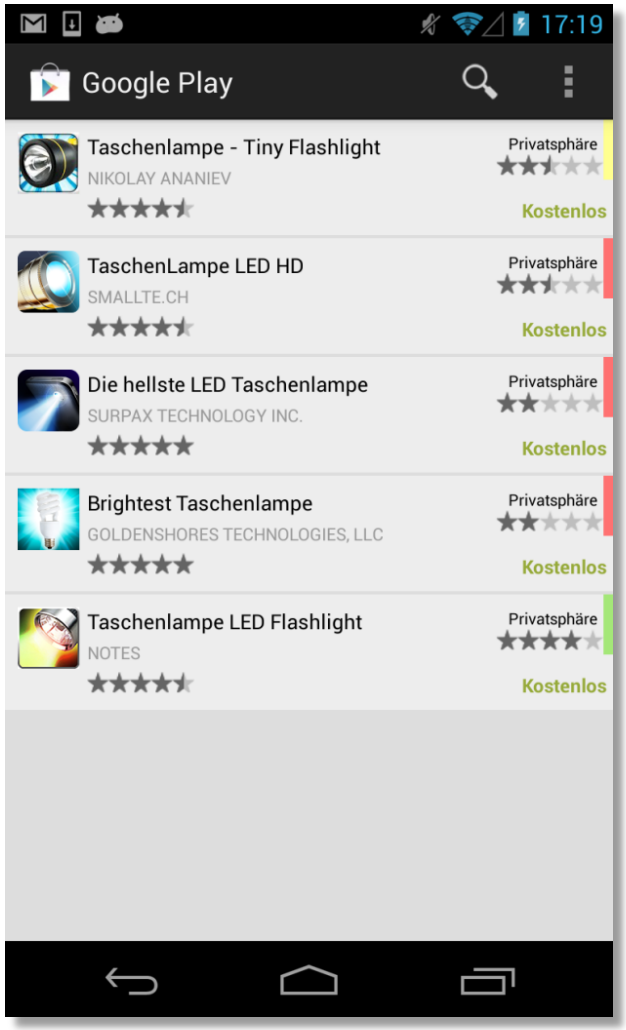
Current privacy risk information is…

- … static,
- … coarse-grained & technical,
- … timed inappropriately,
- … ignored largely,
- … does not support informed decision-making.



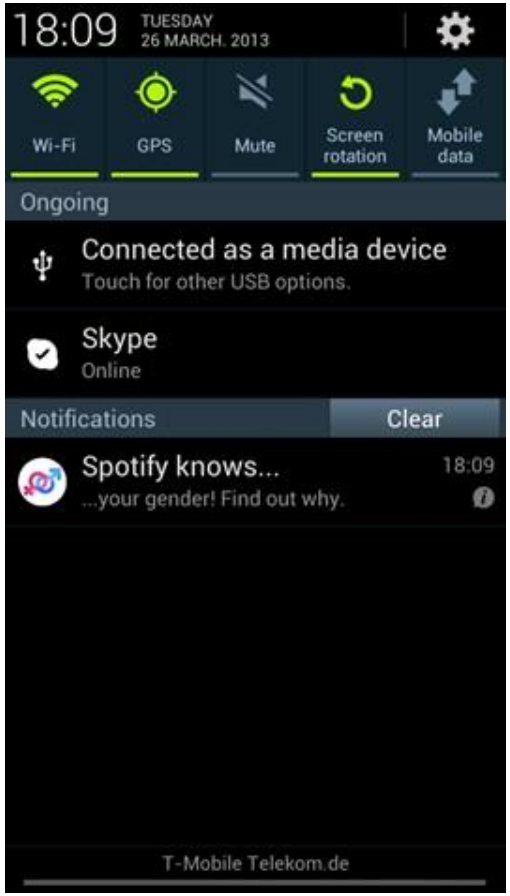
2 The Case of Smartphone Apps

Suggested New Approaches (1/2): Google Play Study



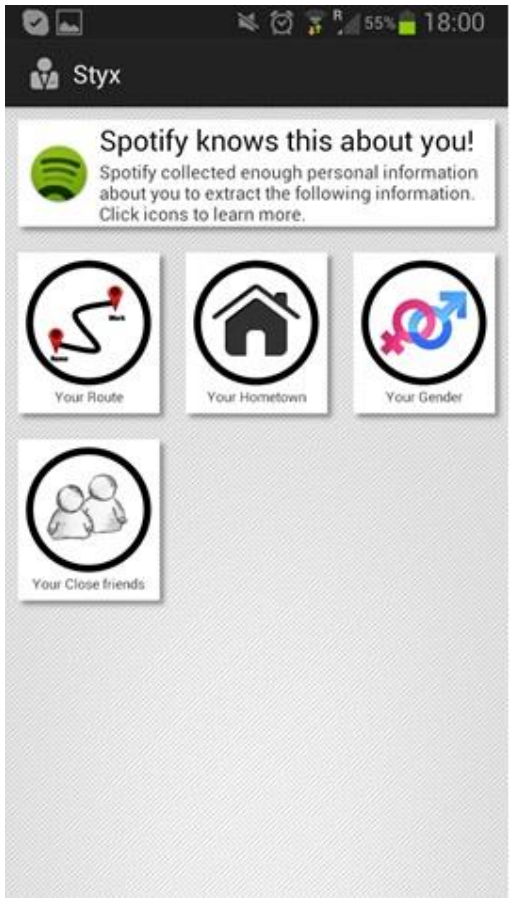
2 The Case of Smartphone Apps

Suggested New Approaches (2/2): Android Study



Styx Notification

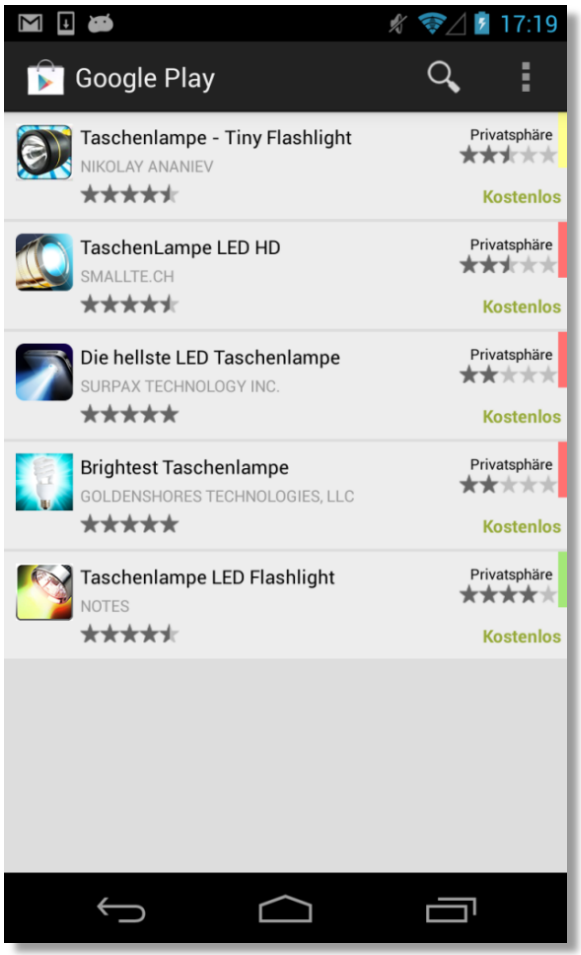
Styx Inference Screen



Styx Dashboard

2 The Case of Smartphone Apps
Results of Two User Studies (Summary)

- A consequence-based privacy-risk communication leads to:
  - increased privacy and risk awareness,
  - better comprehension of risks,
  - better comparison of apps,
  - privacy as a stronger decision factor,
  - safer app choices.



CHALLENGES & RECOMMENDATIONS

3 Challenges & Recommendations
Challenges

Challenge	Description
1. Conceptualization of Privacy Consequences	• Identification and conceptualization of consequences • Consideration of context, scenario, etc. • Positive vs. negative consequences
2. Consider functionality and context of data access	• Consideration of the purpose of an application (“demand level”) • Context of access (e.g. background information flows vs. active UI)
3. Monitor data-access behavior of apps	The actual data-access behavior of an app is significantly influencing the privacy intrusiveness of an app (what resources? how frequent? what combinations? interactions with other apps?); TaintDroid as an example (Enck et al. 2010).
4. Consider Privacy Transparency of App Providers	Privacy-related consequences also depend on how the app provider processes personal data; statements from the app provider such in a privacy policy could be used to determine consequences.
5. Automation	Automation of monitoring and risk assessments will positively influence efficiency, effectiveness, scalability, and costs.

3 Challenges & Recommendations
Recommendations

Who?	What?
Smartphone Platform Providers	Mechanisms to keep track of sensitive-information flows; reason about privacy intrusiveness of apps based on data-access behavior; communicate observed behavior to other potential users.
App Marketplaces	Add more useful privacy information about apps, especially about privacy consequences to support decision-making; add privacy rating for apps based on their data-access profiles and purpose of data access; provide developers with standardized ways to explain permission requests.
App Developers	Provide explanations for permission requests (e.g. core functionality, side functionality, advertisements, etc.).
W3C	Support app developers by standardizing transparency mechanisms in Device API use.

Thank You!

Gökhan Bal, Dipl.-Inf.
Institute of Business Informatics
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
Grüneburgplatz 1, 60629 Frankfurt am Main, Germany
Tel: +49(69) 798-34702, Fax: +49(69)798-35004
Web: http://www.m-chair.de