PADERBORN UNIVERSITY

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

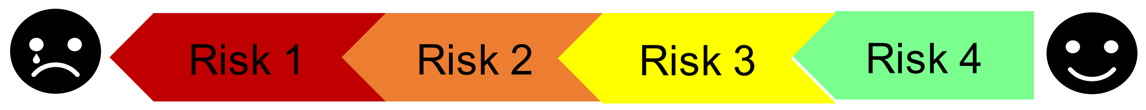
Code Meets Compliance: Statically Visualizing Android Privacy Flows

Mugdha Khedkar[1], Michael Schlichtig[1], and Eric Bodden[1,2]
[1] *Heinz Nixdorf Institute, Paderborn University, Germany,* [2] *Fraunhofer IEM, Paderborn, Germany*

Problem

- Android apps collect and process personal data.
- Privacy by design [1] and GDPR [2] need app developers to use technical measures to protect their users' privacy.
- App developers may need assistance in writing privacy-aware code.
- DPOs, lawyers, and privacy experts lack technical expertise.
- This **gap in expertise** hinders accurate privacy assessments.

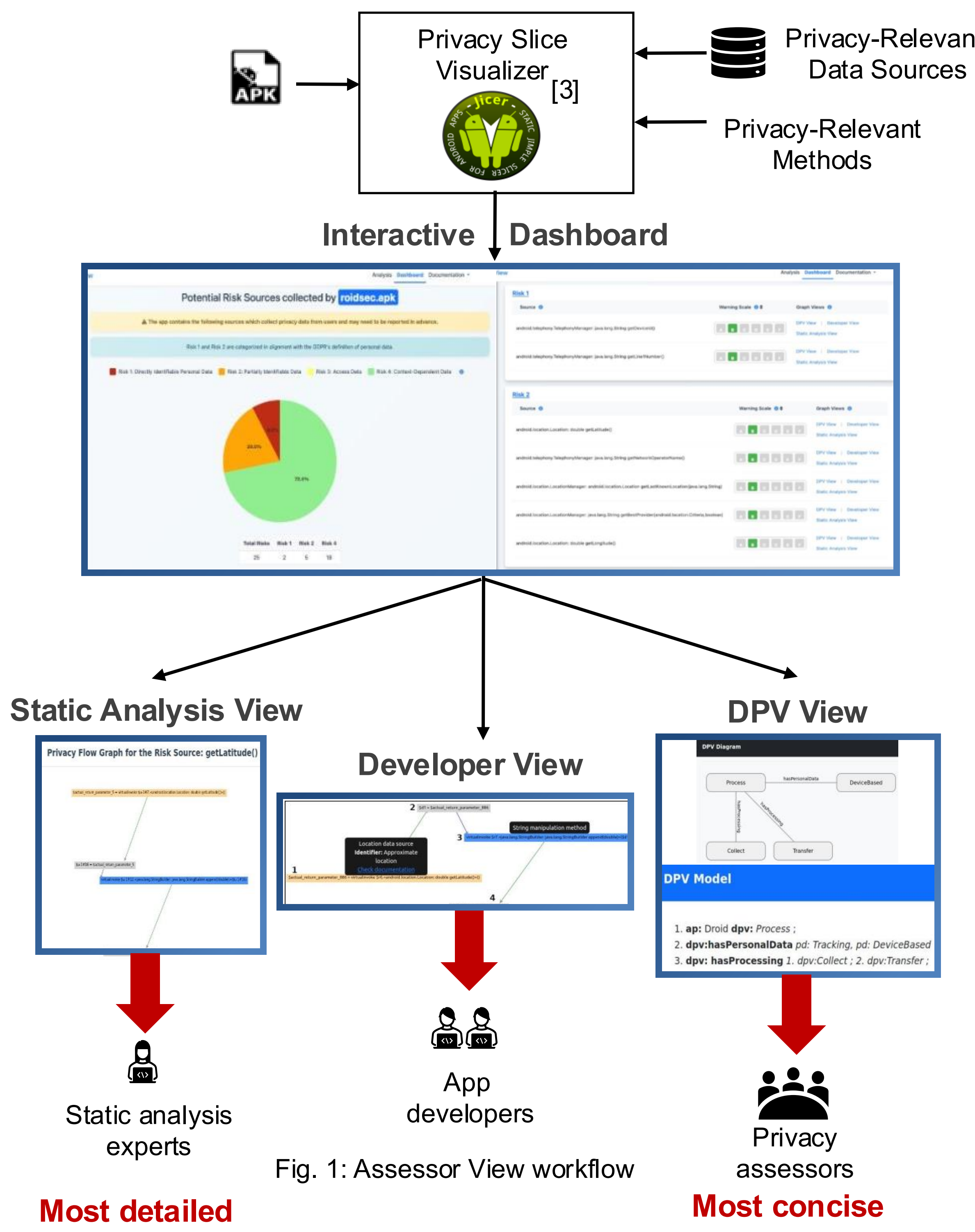
Risky Data Collected by Apps



Directly identifiable data	Partially identifiable data	Access data	Context-dependent data
email ID	first name	password	message

Assessor View

- Uses a static program slicer [3] to preserve control and data dependencies of all *personal data sources.*
- Generates interactive program slices in Jimple and Java for developers.
- Provides a mapping from source code to legal aspects of GDPR, suitable for DPOs, lawyers, and privacy experts.



1. **ap:** Droid **dpv:** *Process ;*
2. **dpv:hasPersonalData** *pd: Tracking, pd: DeviceBased*
3. **dpv: hasProcessing** *1. dpv:Collect ; 2. dpv:Transfer ;*

Fig. 1: Assessor View workflow

Evaluation: Developer Perspectives

- **Study method:** User study with Computer Science students (n = 12)
- **Focus:** Usefulness for understanding app behavior
- **RQ:** *To what extent does the Assessor View help developers understand data protection in Android apps?*

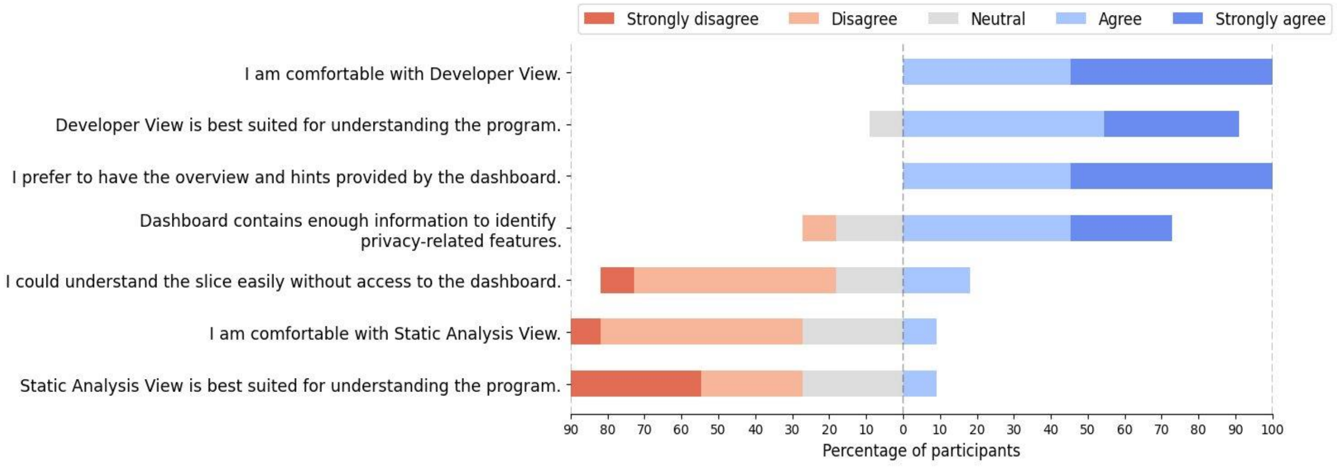


Fig. 2: Participants' experience with the Developer View, and Static Analysis View

Key insight: Assessor View helps developers in understanding privacy-relevant properties of an Android app.

Evaluation: Privacy Experts and DPOs

- **Study method:** Interview-based user study with DPOs, lawyers, privacy experts (n = 16)
- **Focus:** Utility for privacy impact assessments and discussions
- **RQ1:** *How are privacy assessments conducted in a real-world setting?*

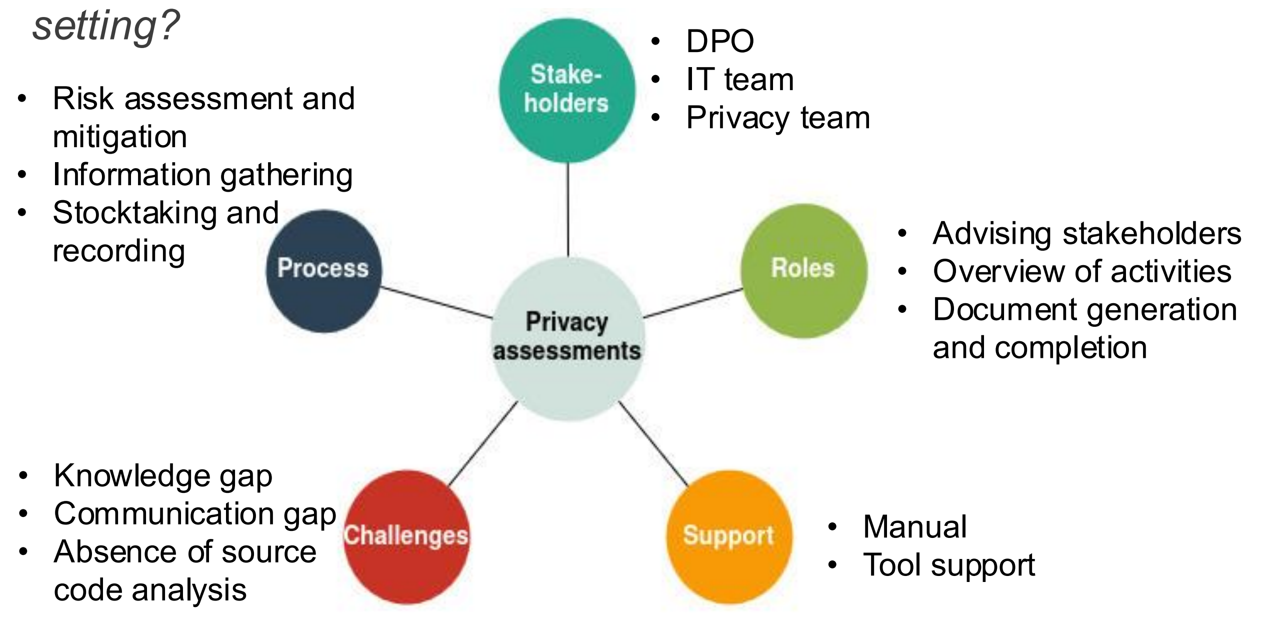


Fig. 3: Themes identified in the interviews

- **RQ2:** *To what extent does the Assessor View support privacy assessors in conducting privacy assessments?*

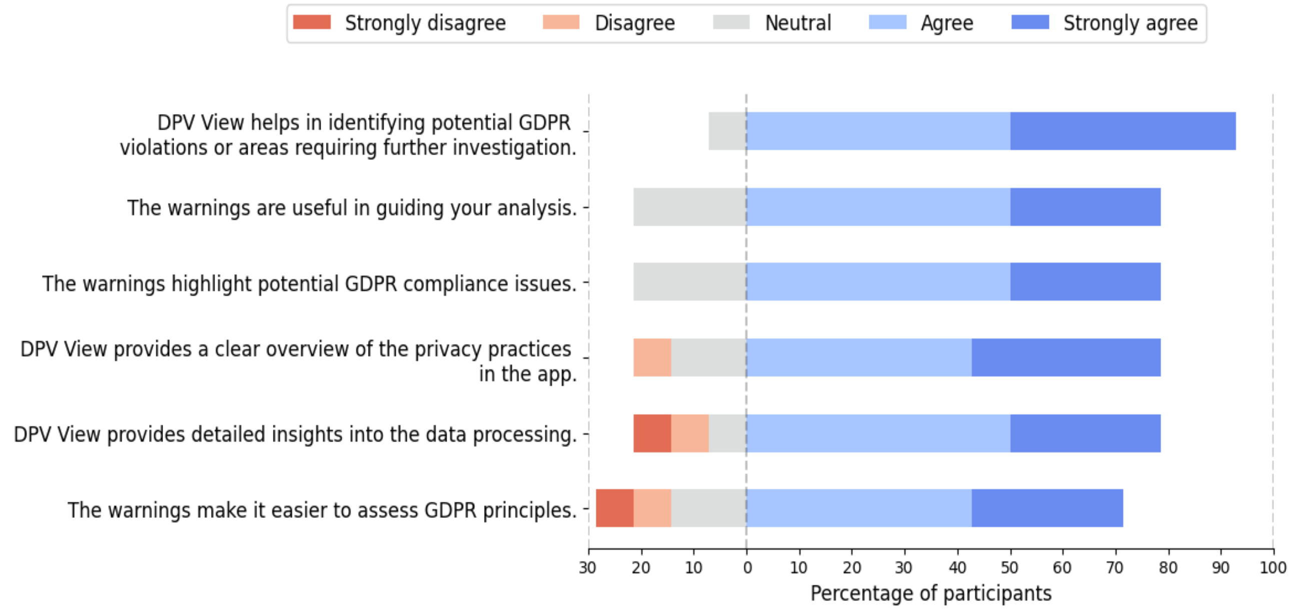


Fig. 4: Participants' experience with the DPV View and GDPR warnings

Key insight: Assessor View is well suited to assist DPOs and privacy experts in their analysis.

[1] Ann Cavoukian et al. 2009. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada 5 (2009), 12
[2] https://eur-lex.europa.eu/legal-content/ EN/TXT/PDF/uri=CELEX:32016R0679
[3] https://foellix.github.io/Jicer/

mugdha.khedkar@uni-paderborn.de

https://mugdhak30.github.io/

SECURE SOFTWARE ENGINEERING GROUP