RestAssured

UNIVERSITÄT DUISBURG ESSEN

Open-Minded

Privacy Policy Specification Framework

for Addressing End-Users Privacy Requirements

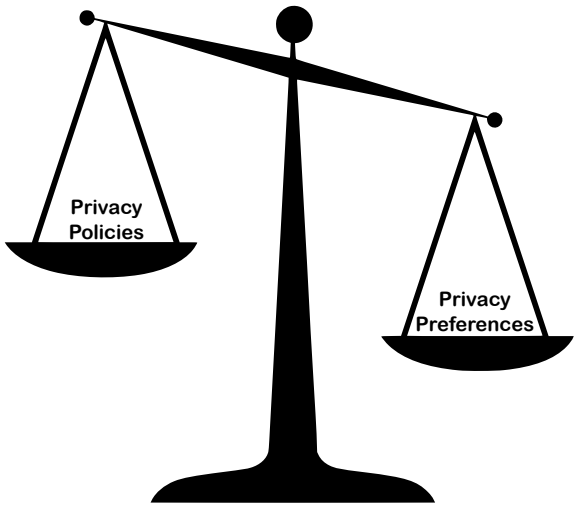
PALUNO
The Ruhr Institute for Software Technology

Nazila Gol Mohammadi, **Jens Leicht**, Nelufar Ulfat-Bunyadi and Maritta Heisel ■ 2019.08.29

Overview
Table of Contents

Introduction

- General Data Protection Regulation (GDPR)
  - Protection of users' privacy
  - Privacy by design/default
  - Transparency
  - Consent in many cases required
  - High fines possible
- Policies are incomprehensible
- Users are overwhelmed with wall of text [3, 6]
- Policies do not support easy withdrawal of consent



"Weight" of Privacy Protection

- Many parties handle users' data for single service
  - Different policies
  - Trustworthiness of parties hard to estimate
- Sticky Policies empower users
  - Too strict policies possible
  - Not user-friendly to define
- Our framework:
  - Uses sticky policies
  - Enables users to adjust policies
  - Ensures service provision stays possible
  - $\Rightarrow$ transparency and intervenability
- Focus on capturing of preferences - not monitoring, nor enforcement

Privacy Policies
Background

- Privacy Policies consist of privacy requirements
- Privacy Requirements refine Privacy Goals
- Textual Privacy Policies consist of statements describing:
  - Handling of data
  - Kind of data collected/processed
  - Obligations of the service provider
  - Actions taken on the data (type of processing)
  - The purpose of the processing
- Legalese difficult to comprehend by users

Privacy Policies - cont.

Background

- Textual Privacy Policies
  - Service-Oriented
  - “Take it or leave it!” principle - select other service provider
  - Not changeable by users

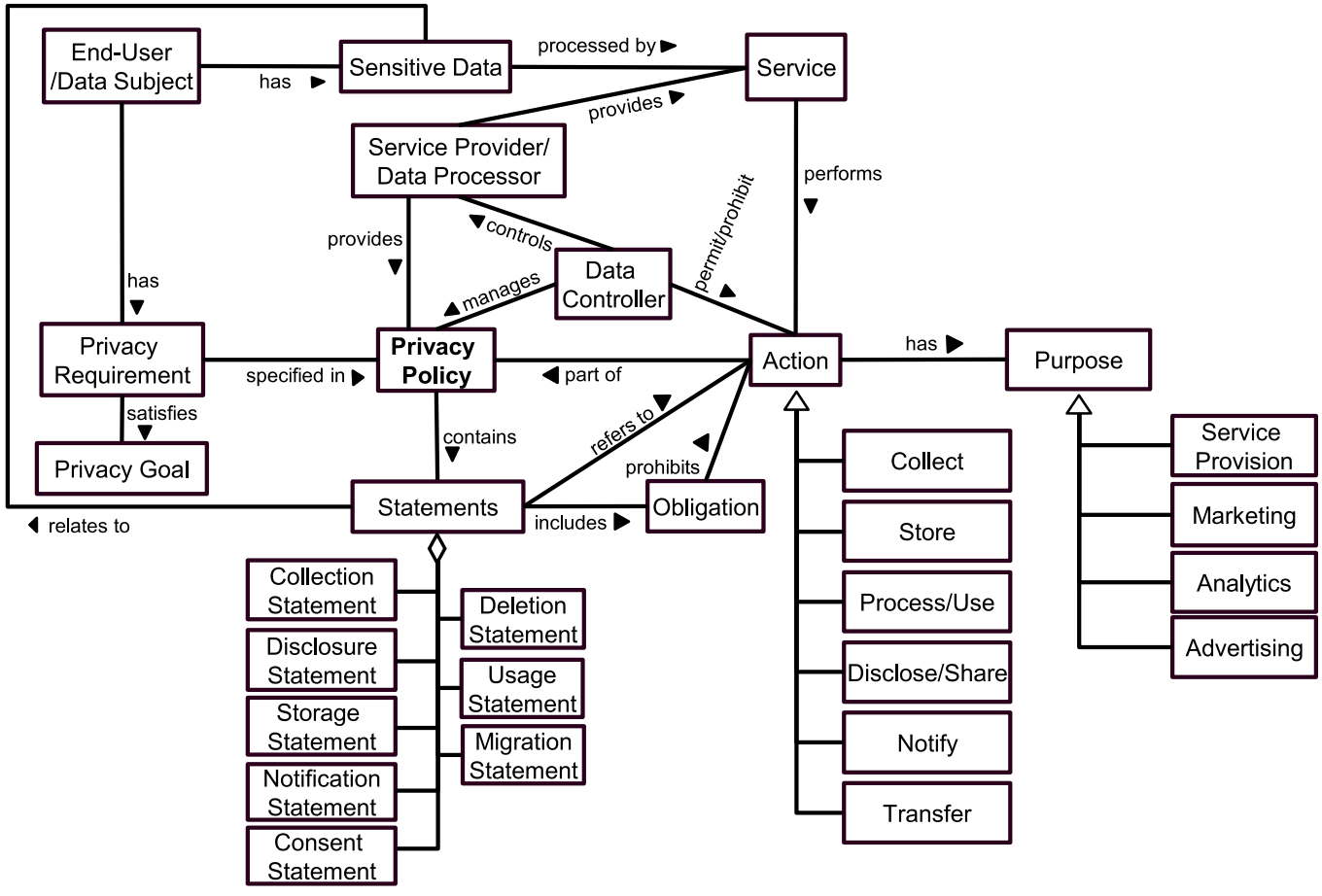
- Sticky Policies [5, 7]:
  - Data-Oriented
  - Users can define policies for their data
  - All parties know how to handle the data
  - Trust-based $\Rightarrow$ Requires trusted authority

Challenges

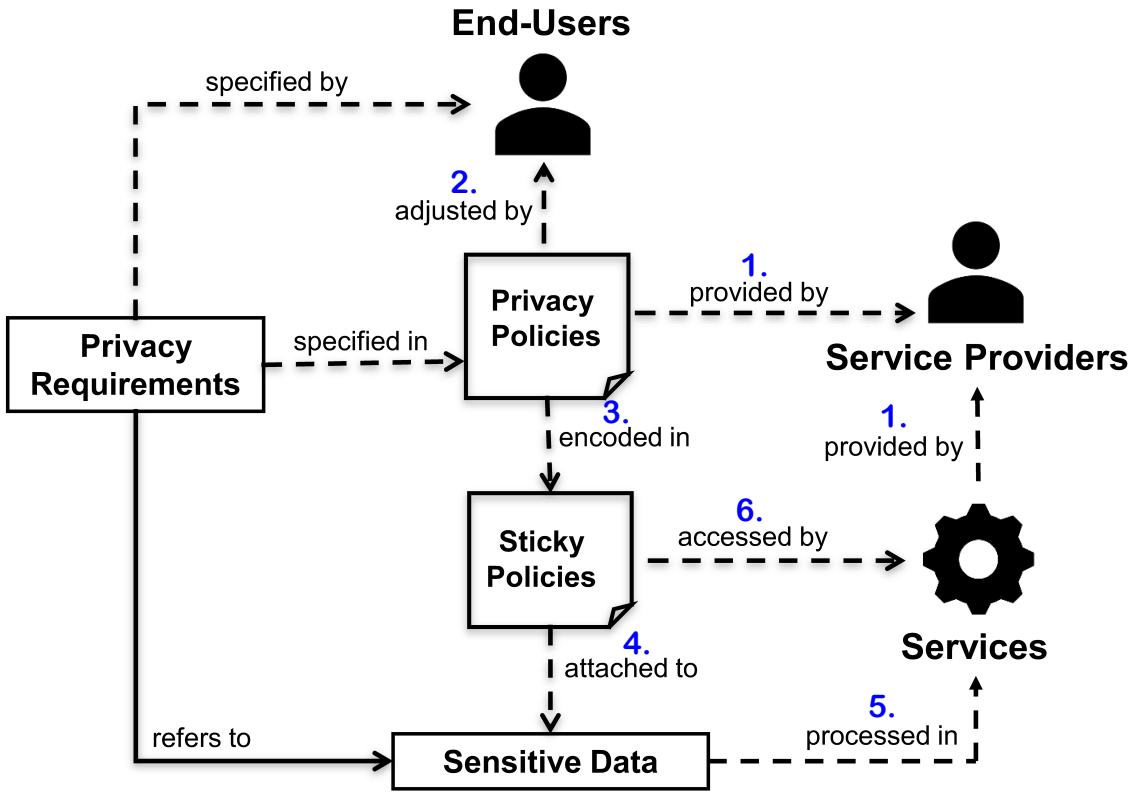
Addressing Users' Privacy Requirements

1. "Take it or leave it!" attitude of service providers
2. Users' lack of knowledge concerning definition of sticky policies
3. Lack of trust in service providers and trusted authorities [sticky policies]
4. Too strict user-defined sticky policies

Conceptual Model



Process of Privacy Policy Handling



Proof of Concept
Example User Interface

- Developed in another work of ours [1]
- Columns represent purposes
- Fixed check marks prevent misunderstanding [service provision]
- Check boxes unchecked by default (“privacy-by-default” - GDPR)
- 4 purposes should be enough:
  - 5th purpose possible: “other”
  - Information about purpose mainly given in description of statement
- 9 categories for type of data
- Green once consent was given

Related Work

- Sticky Policies: + user orientation – service providers' side not considered
- EnCoRe Project: + empowers users – no detailed information available (website offline)
- Pattern for user interface based on "Nutrition Label" by [3]
- Pictograms in context of privacy [2]
- Policy negotiation [4]

Discussion

- Intervenability + Transparency achieved in research:

  $\Rightarrow$ but not simultaneously

- Asymmetry between users and service providers reduced
- 3 out of 4 identified challenges addressed:
  - *"Take it or leave it!"* partially resolved by modifiability, but

    all statements could be assigned the purpose "Service Provision"

    $\Rightarrow$ further addressed by legislation (GDPR)
  - Conceptual user interface resolves *"lack of knowledge for defining sticky policies"*
  - Purpose "Service Provision" prevents *"too strict policies"*
- Enforcement of elicited privacy preferences out of scope

  $\Rightarrow$ Data controllers are expected to have already implemented enforcement mechanisms

Summary

+ More user-oriented privacy policies
+ Better understanding of privacy policies
+ Reduced effort (cf. sticky policies) for users

Future Work

- Implementation of all functionalities
- Evaluation through case studies

  $\Rightarrow$ Experiments with users
- Prevent service providers from misuse of “service provision” purpose

Thank you

for your attention!

Questions or comments?

Bibliography I


Gol Mohammadi, N., Pampus, J., Heisel, M.: Resolving the conflicting needs of service providers and end-users: A pattern for incorporating end-users privacy preferences into privacy policies (2019), submitted for publication


Hansen, M.: Putting privacy pictograms into practice-a european perspective. GI Jahrestagung **154**, 1–703 (2009)


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. p. 4. ACM (2009)


Kolter, J.P.: User-centric Privacy: A Usable and Provider-independent Privacy Infrastructure, vol. 41. BoD–Books on Demand (2010)


Pearson, S., Casassa-Mont, M.: Sticky policies: an approach for managing privacy across multiple parties. Computer **44**(9), 60–68 (2011)

Bibliography II


Pollmann, M., Kipker, D.K.: Informierte einwilligung in der online-welt. Datenschutz und Datensicherheit-DuD **40**(6), 378–381 (2016)


Spyra, G., Buchanan, W.J., Ekonomou, E.: Sticky policies approach within cloud computing. Computers & Security **70**, 366–375 (2017)


Zwingelberg, H., Hansen, M.: Privacy protection goals and their implications for eid systems. In: IFIP PrimeLife International Summer School on Privacy and Identity Management for Life. pp. 245–260. Springer (2011)