Privacy Policy Specification Framework
for Addressing End-Users Privacy Requirements

Nazila Gol Mohammadi, Jens Leicht, Nelufar Ulfat-Bunyadi and Maritta Heisel  ■ 2019.08.29
Overview
Table of Contents

Introduction

Background

Privacy Policy Specification Framework

Related Work

Conclusion and Future Work
Introduction

Background

Privacy Policy Specification Framework

Related Work

Conclusion and Future Work
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
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
Introduction

Background
  - Privacy Policies

Privacy Policy Specification Framework

Related Work

Conclusion and Future Work
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
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 ⇒ Requires trusted authority
Introduction

Background

Privacy Policy Specification Framework

- Challenges
- Conceptual Model
- Process of Privacy Policy Handling
- Proof of Concept

Related Work

Conclusion and Future Work
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
Process of Privacy Policy Handling

1. Privacy Policy Specification Framework
2. 2019.08.29
3. swe.uni-due.de
4. 12/22
- 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

Overview

Introduction

Background

Privacy Policy Specification Framework

Related Work

Conclusion and Future Work
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]
Introduction

Background

Privacy Policy Specification Framework

Related Work

Conclusion and Future Work

- Discussion
- Summary
- Future Work
Discussion

- Intervenability + Transparency achieved in research:
  ⇒ 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”
    ⇒ 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
  ⇒ 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
  ⇒ Experiments with users
- Prevent service providers from misuse of “service provision” purpose
Thank you
for your attention!

Questions or comments?
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


