

UCLrvine

Institute for Software Research

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization

Yang Wang and Alfred Kobsa
University of California, Irvine, USA

UM05 Workshop on Privacy-Enhanced Personalization Edinburgh, Scotland

UCLrvine

Institute for Software Research

outline

- motivation
- software product line
- our privacy-enabling user modeling architecture
- an example
- conclusion


A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEP05 Yang Wang and Alfred Kobsa 2

UCLrvine

Institute for Software Research

motivation

- web personalization benefits both customers and vendors
- privacy concerns counteract the personalization benefits
- how to dynamically balance personalization and privacy?



A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEP05 Yang Wang and Alfred Kobsa 3

UCLrvine

Institute for Software Research

aims and key characteristics

- provide optimal personalization while respecting privacy laws, regulations and users' personal privacy preferences
- leverage the flexibility of software product line to address combinatorial complexity of privacy constraints
- apply state-of-the-art industry practice for managing software variants at run time


A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEP05 Yang Wang and Alfred Kobsa 4

UCLrvine

Institute for Software Research

UniversalFriends.com

- bridge physical distances
- foster universal friendship
- recommend personalized list of likely friends



A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEP05 Yang Wang and Alfred Kobsa 5

UCLrvine

Institute for Software Research

privacy concerns

complex combinations of:

- users' personal privacy preferences
- international privacy laws (even trans-border)
- privacy regulations

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEP05 Yang Wang and Alfred Kobsa 6

Institute for Software Research UCLrvine

users' privacy preferences

"only collect my information if I give explicit consent !"

"do not store my true name !"

"do not track me !"

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 7

Institute for Software Research UCLrvine

privacy laws

- EU data protection directive
- Asia-Pacific Economic Cooperation (APEC) privacy framework
- Organisation for Economic Co-operation and Development (OECD) privacy guidelines
- over 30 countries already have their own privacy laws and more countries are coming

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 8

Institute for Software Research UCLrvine

data protection laws – year 2003

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 9

Institute for Software Research UCLrvine

privacy regulations

- sector standards (e.g., in USA)
 - medical: HIPAA
 - children: COPPA
 - finance: Gramm-Leach-Bliley Act
- self-regulation policies
 - TRUST e
 - Network Advertising Initiative
 - Chinese E-Commerce Trust Consortium

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 10

Institute for Software Research UCLrvine

the research question

how can personalized web-based systems maximize the personalization benefits while at the same time being compliant with the privacy constraints that are currently in effect?

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 11

Institute for Software Research UCLrvine

revisit the research question

seeking a mechanism to dynamically select user modeling components that comply with the currently prevailing privacy constraints

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 12

Institute for Software Research UCLrvine

user modeling component pool

user modeling component	methods used	data used		
		demographic data	user-supplied data	visited pages
UMC ₁	clustering	X		
UMC ₂	rule-based reasoning		X	
UMC ₃	fuzzy reasoning with uncertainty		X	
UMC ₄	rule-based reasoning	X	X	
UMC ₅	fuzzy reasoning with uncertainty	X	X	
UMC ₆	incremental machine learning		X	X
UMC ₇	one-time machine learning		X	XXX
UMC ₈	one-time machine learning + fuzzy reasoning with uncertainty	X		XXX

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 13

Institute for Software Research UCLrvine

product line architecture

- "The common architecture for a set of related products or systems developed by an organization." [Bosch, 2000]
- a PLA includes
 - ▶ Stable core: basic functionalities
 - ▶ Options: optional features/qualities
 - ▶ Variants: alternative features/qualities
- A particular architecture *instance* is *selected* from the product-line architecture

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 14

Institute for Software Research UCLrvine

our approach

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 15

Institute for Software Research UCLrvine

an example

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 16

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 18

Institute for Software Research UCLrvine

the privacy constraints

Privacy constraints applied to Alice

German Tele-Service Data Protection Law

Section 4(2)-(4): profiling

Combining user profiles retrievable under pseudonyms with data relating to the content of the pseudonym is prohibited.

Personal data to be erased immediately after each session except for very limited purposes.

Privacy constraints applied to Cheng

Cheng's own privacy preferences:

"Dislike being tracked"

Privacy constraints applied to Bob

Network Advertising Initiative (NAI) Self-Regulatory Principles

Section B: NAI's Statement of Purposes

Merging non-personally identifiable site data with personally identifiable demographic data is prohibited unless user gives prior affirmative consent.

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 18

Institute for Software Research UCIrvine

conclusions

- provide optimal personalization while respecting privacy laws, regulations and users' personal privacy preferences
- leverage the flexibility of software product line to address combinatorial complexity of privacy constraints
- apply state-of-the-art industry practice for managing software variants at run time

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 19

Institute for Software Research UCIrvine

project status and future work

- currently prototyping the system
- systematically express privacy constraints
- a decentralized version
- privacy kernel

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 20

Institute for Software Research UCIrvine

acknowledgements

- Alfred Kobsa
- André van der Hoek
- Eric Dashofy
- Yun Huang
- Norman Su
- Colleagues at CommerceNet

A Software Product Line Approach for Handling Privacy Constraints in Web Personalization PEPOS Yang Wang and Alfred Kobsa 21