

The Role of Policy and Stakeholder Privacy Values in Requirements Engineering

Annie I. Antón
Thomas A. Alspaugh
Julia B. Earp
Colin Potts

IEEE Int'l Symposium on Requirements Engineering
Toronto, Canada
August 30, 2001

E-Commerce Studio
NORTH CAROLINA STATE UNIVERSITY

Objective

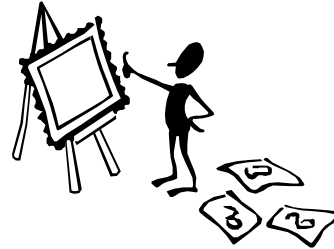
Encourage adoption of a more holistic view of application and specification, in which system or application is seen as an engine of policy enforcement and values attainment.

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
NORTH CAROLINA STATE UNIVERSITY

Agenda

- ❑ Background
- ❑ The Role of Policy in RE
- ❑ Privacy Goals
- ❑ Physical Privacy Metaphors
- ❑ Summary and Future work



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Privacy and Privacy Policies

- ❑ Privacy
 - The right to be let alone
 - Control over what information about you is revealed, and to whom
- ❑ Privacy Policy
 - A comprehensive description of a Web site's practices that is located on the site itself and may be easily accessed by visitors [FTC98]

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Common Policy Problems

- ❑ Nonconformance to “standard”
 - Organisation for Economic Cooperation & Development
 - Federal Trade Commission
 - Fair Information Practices
- ❑ Ambiguity and misplaced trust
 - Policies are difficult to find/interpret
- ❑ Failure to implement policy
 - Inconsistencies are common

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
NORTH CAROLINA STATE UNIVERSITY



- ❑ A TRUSTe licensee's privacy policy must disclose:
 - *what* personal information is being gathered;
 - *how* the information will be used;
 - *who* the information will be shared with;
 - the *choices* available regarding how collected information is used;
 - *safeguards* in place to protect personal information from loss, misuse, or alteration; and
 - how individuals can *update or correct* inaccuracies in information collected about them.

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
NORTH CAROLINA STATE UNIVERSITY

Toysmart

- ❑ Policy: no sharing of PI w/ 3rd parties
- ❑ *Wall Street Journal* ad to sell DB after going out of business last May
- ❑ Internet privacy activists protested
 - if the sale of that information were allowed, it could encourage a wave of other failing dot-coms to abandon privacy assurances in return for cash.
- ❑ Landmark case
 - privacy promises made while in business must be kept when you go out of business

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

The Problem

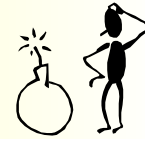
- ❑ Software systems fail to adequately address security and privacy issues during analysis & design.
- ❑ We (“Requirements Engineers”) have failed to apply our methods to generate privacy and security policies as well as the corresponding requirements.



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Challenges



- ❑ Traditional RE techniques difficult to apply when:
 - rapidly changing technologies change policies
 - external pressure exists to disclose practices
- ❑ Need for prescriptive guidance to develop policy requirements [Trcek, PFIRES]
 - Security policy
 - Privacy policy

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Role of Policy in RE: Policies vs. Requirements

- ❑ Similarities
 - express desire or worth, rather than fact
 - primarily statements in the optative mood, they specify what must or ought to be done
- ❑ Differences
 - scope of policies is broader than requirements
 - privacy policies are more charged w/ societal values
 - policies are more open-ended than requirements
 - requirements cover one system; policies cover several
- ❑ Alignment
 - bringing policy and requirements into agreement

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Goal-Based Specification

- ❑ Teleological models - directed goal network
 - Goals, subgoals, actors, obstacles
- ❑ Strategic Goals
 - reflect high-level enterprise goals / long term, broad based initiatives
- ❑ Tactical Goals
 - involve short term goal achievement

Focusing on goals rather than requirements allows us to communicate with stakeholders in terms of their values

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
WYOMING STATE UNIVERSITY

Scenario-Based Analysis



- ❑ Envisage how technical systems may change as a result of socio-technical changes
- ❑ Bringing tactical goals into alignment with the organization's strategic goals

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
WYOMING STATE UNIVERSITY

Scenarios

- ❑ Use cases
 - illustrate actual or desired sequences of satisfactory events
- ❑ Abuse cases
 - interventions lead to policy violation
 - security intrusion
 - disclosing information to 3rd party w/o permission
- ❑ Misuse cases
 - willful undermining of a policy
 - using information for purpose for which it is not intended

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
HEALTH CARE UNIVERSITY

Aligning Values with Systems & Policy

- ❑ Policies developed as an afterthought
- ❑ Many e-commerce systems fail to address consumer privacy values and concerns
- ❑ How do values affect system evolution and IT policy?
- ❑ Use goals to:
 - analyze conflicts w/ policies & corresponding web sites
 - Reconstruct implicit requirements met by privacy policies



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
HEALTH CARE UNIVERSITY

Goal Mining for Privacy Requirements

□ Goal mining

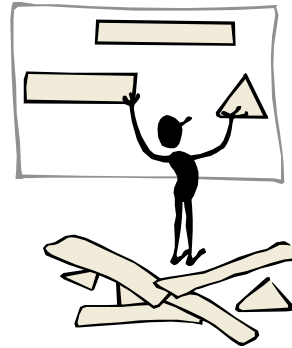
- extracting pre-requirements goals from post-requirements text artifacts
- reconstruct the implicit requirements met by the privacy policies

□ Taxonomy:

- Privacy Protection Goals
- Privacy Vulnerability Goals
- Respective Requirements

□ Goal:

- Library of stable, reusable privacy and security goals for *SMaRT*



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Privacy Policy Analysis #1

□ ISPs

- AOL
- Earthlink
- Free Internet

□ Online Retailers

- Amazon
- eNews
- ToySmart

□ Traditional M.O. Catalog

- Banana Republic
- Eddie Bauer
- JCrew

□ Auction Sites

- Ebay
- Reverse Auction
- Sothebys

□ Drug Stores

- Drugstore.com
- Eckerd Drugs
- Long Drugs

□ Grocery Stores

- HomeGrocer
- Lowes
- Peapod

□ Travel Agencies

- American Express
- Expedia
- Travelocity

□ Trust Services

- BBBOnline
- TRUSTe
- Verisign



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Privacy Policy Analysis #2

❑ Pharmaceuticals

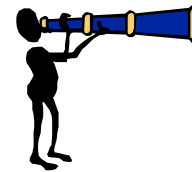
- Bayer
- Glaxo Wellcome
- Eli Lilly
- Novartis (Ciba)
- Pfizer
- Pharmacia & Upjohn

❑ Drug Stores

- Corner Drugstore
- DestinationRx
- Drugstore
- Eckerd
- Health Allies
- Health Central
- iVillage
- Prescription Online
- WebRX

❑ Health Insurance

- AETNA
- AFLAC
- BCBS
- CIGNA
- eHealth Insurance
- Kaiser Permanente
- Online Health Plan



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
HEALTH CARE AND STATE UNIVERSITY

Taxonomy

❑ Privacy Protection Goals

- Access/Participation
- Choice/Consent
- Enforcement/Redress
- Integrity/Security
- Notice/Awareness

❑ Privacy Vulnerability Goals

- Aggregation of Information
- Collection of Information
- Monitoring of Information
- Personalization
- Solicitation
- Storage of Information
- Transfer of Information



© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
HEALTH CARE AND STATE UNIVERSITY

Privacy Protection Goals

- ❑ **Notice/Awareness**
 - NOTIFY users before data is collected
 - NOTIFY users of updates to privacy policy
- ❑ **Choice/Consent**
 - ALLOW customer to opt-in to sharing PII w/ member sites
 - OPT-IN to controlling whether to have PII stored
- ❑ **Access/Participation**
 - ALLOW customer to check their PII for accuracy
 - ALLOW customer to modify their PII
- ❑ **Integrity/Security**
 - CROSS-REFERENCE user info to find uses of multiple IDs or aliases
- ❑ **Enforcement/Redress**
 - DISCIPLINE associates/employees who violate privacy policy

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
EAST CAROLINA STATE UNIVERSITY

Potential Privacy Invasions

- ❑ **Collection of Information**
 - COLLECT children's names and ages when they enter contests
 - COLLECT user browsing patterns
- ❑ **Monitoring of Information**
 - MONITOR customer site usage patterns
- ❑ **Personalization**
 - CUSTOMIZE offers based on customer's account and purchase records
- ❑ **Storage of Information**
 - STORE purchase records
- ❑ **Aggregation of Information**
 - AGGREGATE purchase info by zip code
- ❑ **Transfer of Information**
 - SHARE PII w/ third parties

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
EAST CAROLINA STATE UNIVERSITY

Summary: Addressing the Problem

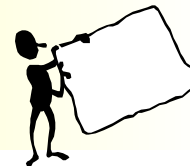


- ❑ Need to establish effective approaches for privacy and security requirements coverage
- ❑ Apply scenario management and goal-driven analysis strategies
- ❑ Apply metaphor analysis [Potts - RE'01]
- ❑ Ensure system requirements align with organizational policies

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Recommendations & Future Work



- ❑ Studying values and perceptions of online consumers in conjunction with a requirements methodology => alignment
- ❑ Design systems that reflect values and protect our personal information
- ❑ Develop mechanisms to ensure that systems comply with policy
- ❑ Systematically analyze web policies and elucidate values ascribed to them

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
LEHIGH UNIVERSITY

Acknowledgements

- ❑ National Science Foundation

- ❑ Undergraduate Students:
 - Ha To, Santa Clara University (2000)
 - Angela Reese, University of Dayton (2001)

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
SANTA CLARA UNIVERSITY

Thank you!

- ❑ Questions?

© A.I. Antón, J.B. Earp, C. Potts, T.A. Alspaugh, August 2001

E-Commerce Studio
SANTA CLARA UNIVERSITY