

Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems

Marc Langheinrich

Professor Università della Svizzera italiana (USI) in Lugano,
Switzerland

1

Introduction

- **Growth of Internet and E Commerce**
 - Increased use of credit cards
 - paying bills, ordering food done online
 - Requires a lot of user information
 - How and where is that information stored
 - Who has access
 - How long is this data kept

2

Privacy

- 'the right to select what personal information about me is known to what people'



Bo Peep (Lost her sheep but found them right away with her GPS tracking device).

3

Privacy:



"Take these and keep the location app on – the boss said he might need to know where we are".

4

Paper

- **Motivation:**
 - Ubiquitous devices are expected to disappear
 - Capture user specific information
 - Privacy
 - legal subject
 - Ethical issue – subjective
- **Conflicting goals**
 - Privacy
 - Ubiquitous Environments
- **Guidelines to develop ubiquitous devices**

5

Privacy Over the years

- Hot topic for several years.
- **The Right to Privacy**
 - Written by Louis Brandeis and Samuel D. Warren in 1890 in Harvard Journal
 - the printing press / photography
- **Data Protection Laws**
 - 1960
 - Nazi exploitation of public records in World War II

6

Kinds of Privacy

- Behavioral or Media Privacy
 - peeping toms and eaves droppers
- Territorial Privacy
 - Setting limits on intrusion in environments
 - e.g. workplace or public space searches
- Communication Privacy
 - security and privacy of mail, telephones, e-mail
 - Olmstead vs. United States in 1928
 - National Prohibition Act - selling illegal liquors.
 - *Katz v. United States*
 - public pay phone to transmit illegal gambling wagers
- Information Privacy
 - collection and handling of personal data
 - E.g. credit information, medical, government records.

7

Some of the Laws that impacted Privacy

- US Privacy Act of 1974
 - political economist Alan Westin
- EU Directive 95/46/EC of 1995

8

Fair Information Practices

- Openness and transparency
 - No secret record keeping
- Individual participation
 - Subject can see and correct his record
- Collection limitation
 - Information collected proportional to purpose
- Data quality
 - Relevant data
- Use limitation
 - Used for specific purpose by authorized personnel.
- Reasonable security
 - Security level should be according to sensitivity of data
- Accountability
 - People in charge should be accountable

9

EU Directive 95/46/EC

- Limits data transfers to non-EU countries
 - Adequate level of privacy protection
- Subsumes fair information practices
- *Explicit consent*

10

Does Privacy Matter?

- Yes, it does...case by case
- In case of an accident
 - medical records
 - Good for individuals
- FBI is able to decipher secret email
 - terrorist attacks
 - Good for Society
- Centralized power controls access
 - not abuse their powers.
- Everyone will be watching each other

11

Social Implications of Ubiquitous Devices

- Ubiquity
 - Present every where
 - Decisions affect every part of life
- Invisibility
 - interacting/under surveillance
- Sensing
 - Sensors pick up emotions
 - High quality audio and video
- Memory amplification
 - Record every action of us and our surrounding
 - Search through our past
- Lawmakers, sociologists may not be aware of the technology
 - Its up to the designers of systems.

12

Goals and Focus of Research

- Cannot provide total security/privacy
- Goal is to prevent unwanted accidents
- Build relationships based on mutual trust and respect.

13

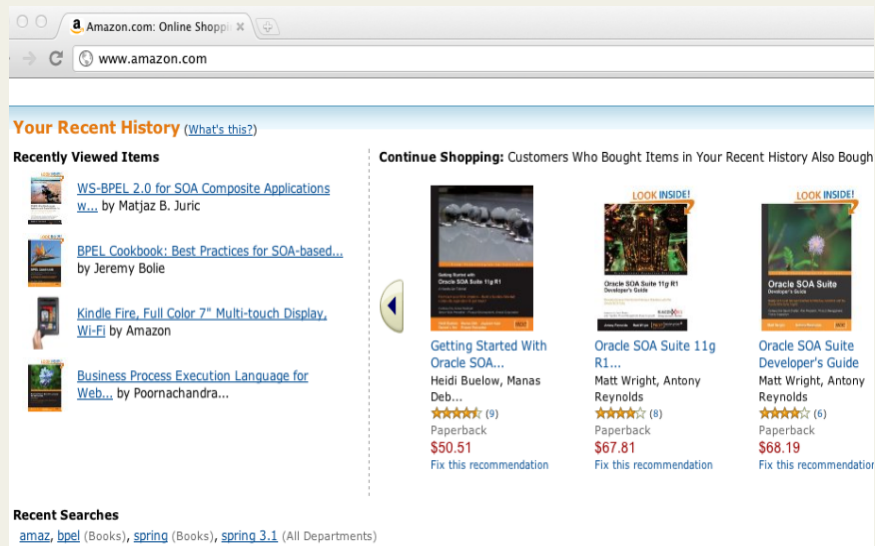
Notice

Stores place signs informing users



14

Notice



The screenshot shows the Amazon.com 'Your Recent History' page. The browser address bar displays 'www.amazon.com'. The page is divided into two main sections: 'Recently Viewed Items' and 'Continue Shopping: Customers Who Bought Items in Your Recent History Also Bought'.

Recently Viewed Items:

- [WS-BPEL 2.0 for SOA Composite Applications](#) by Matjaz B. Juric
- [BPEL Cookbook: Best Practices for SOA-based...](#) by Jeremy Bolie
- [Kindle Fire, Full Color 7" Multi-touch Display, Wi-Fi](#) by Amazon
- [Business Process Execution Language for Web...](#) by Poornachandra...

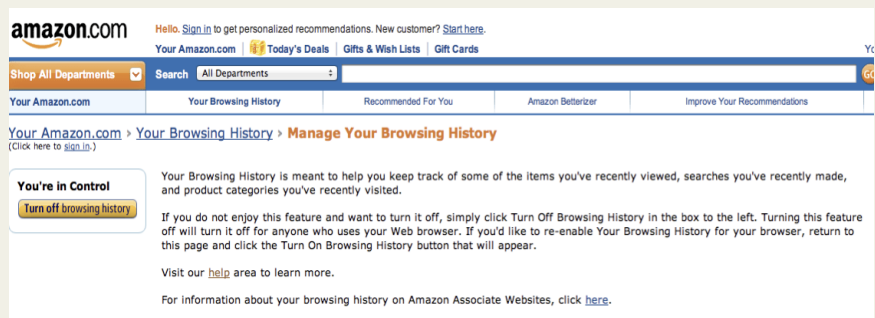
Continue Shopping:

- Getting Started With Oracle SOA...** by Heidi Buelow, Manas Deb... (9 reviews) Paperback \$50.51
- Oracle SOA Suite 11g R1...** by Matt Wright, Antony Reynolds (8 reviews) Paperback \$67.81
- Oracle SOA Suite Developer's Guide** by Matt Wright, Antony Reynolds (6 reviews) Paperback \$68.19

Recent Searches: amaz, bpe (Books), spring (Books), spring 3.1 (All Departments)

15

Notice



The screenshot shows the Amazon.com 'Manage Your Browsing History' page. The top navigation bar includes the Amazon logo, a sign-in prompt, and links for 'Your Amazon.com', 'Today's Deals', 'Gifts & Wish Lists', and 'Gift Cards'. The breadcrumb trail reads: 'Your Amazon.com > Your Browsing History > Manage Your Browsing History'.

You're in Control

[Turn off browsing history](#)

Your Browsing History is meant to help you keep track of some of the items you've recently viewed, searches you've recently made, and product categories you've recently visited.

If you do not enjoy this feature and want to turn it off, simply click Turn Off Browsing History in the box to the left. Turning this feature off will turn it off for anyone who uses your Web browser. If you'd like to re-enable Your Browsing History for your browser, return to this page and click the Turn On Browsing History button that will appear.

Visit our [help](#) area to learn more.

For information about your browsing history on Amazon Associate Websites, click [here](#).

16

Notice

- Data collection
 - known to the subject that is being monitored
- Scenario: memory-amplifier-coffee-cup
- Should have a well known location for publishing such information
 - Robots.txt
 - Emergency frequencies
 - Radio announcements for buildings
- Limitations depending on device
 - power consumption
 - RFID tags
- P3P
 - Which information the server stores
 - Use of this information
 - How long is it stored
- Inform occupants of a building that audio recording is done
- Pay attention to restrictions on surveillance such as wiretapping or video recording

17

Choice and Consent



18

Choice and Consent

- Data collectors
 - receive *explicit consent* from the data subject
- Explicit consent - written contract
- Explicit consent in digital world
 - public-key cryptography
 - Was user aware or did a system do it automatically
- Ubiquitous setting:
 - Devices may not support a tactile interface
 - Unusable
- Notion of consent
 - If only one option available
 - restrictions on purpose, use, and retention of such video feeds
- Offer reason for collecting information
 - If user declines, selectively disable functionality for this user

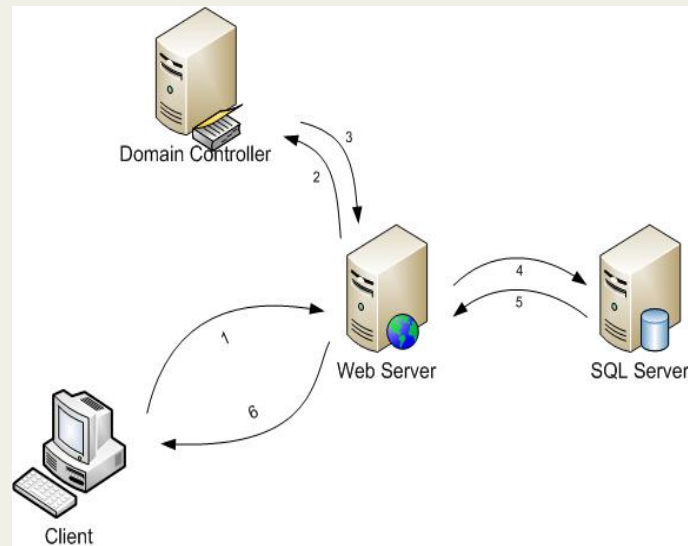
19

Anonymity



20

Pseudonymity



21

Anonymity and Pseudonymity

- Legally collect information without explicit user consent
- Anonymity = not identifiable within a set of subjects
- Difficult in ubiquitous environment
 - video camera can get a clear picture of a person
 - personalization
- Pseudonymity – assigns certain ID to a certain individual
 - Has option to step out of that role
- Issues
 - Can some data be traced back to a person
 - Ex: Data Mining

22

Proximity and Locality

- Proximity
 - data is collected by a device only when the owner is present
 - use biometry
 - Concern : friends playing their recordings to a group of strangers
- Locality
 - Information collected should not leave a particular area
 - Information collected in a building would stay within the building's network
 - Concern: once present, no additional authentication would be required anymore

23

Adequate Security

- Ubiquitous devices present new challenges
 - Power consumption
 - Communication protocols
 - Key distribution and Management
- Robust security
 - highly sensitive data
- Principle of Proportionality
 - Hacking for something worth \$10
- Proximity and Locality
 - Sending information locally, without encryption

24

Access and Recourse

- Separate acceptable from unacceptable behavior
 - detecting violations and enforcing the penalties
- Technology should assist in implementing legal requirements
 - use limitation, access, or repudiation.
- Data Collectors
 - privacy aware technology implemented.
- Allow data subjects to have access to their information
- The principles of Collection and Use Limitation
 - collect data for a well-defined purpose
 - only collect data relevant for the purpose (not more)
 - only keep data as long as it is necessary for the purpose

25

Take Away

- Good Introduction for Software Developers
- Use of Principles in Development of a product
- Consult Legal advisor
 - development of a product

26

Orwellian nightmare



27

Any Questions?

- Thank you!

28