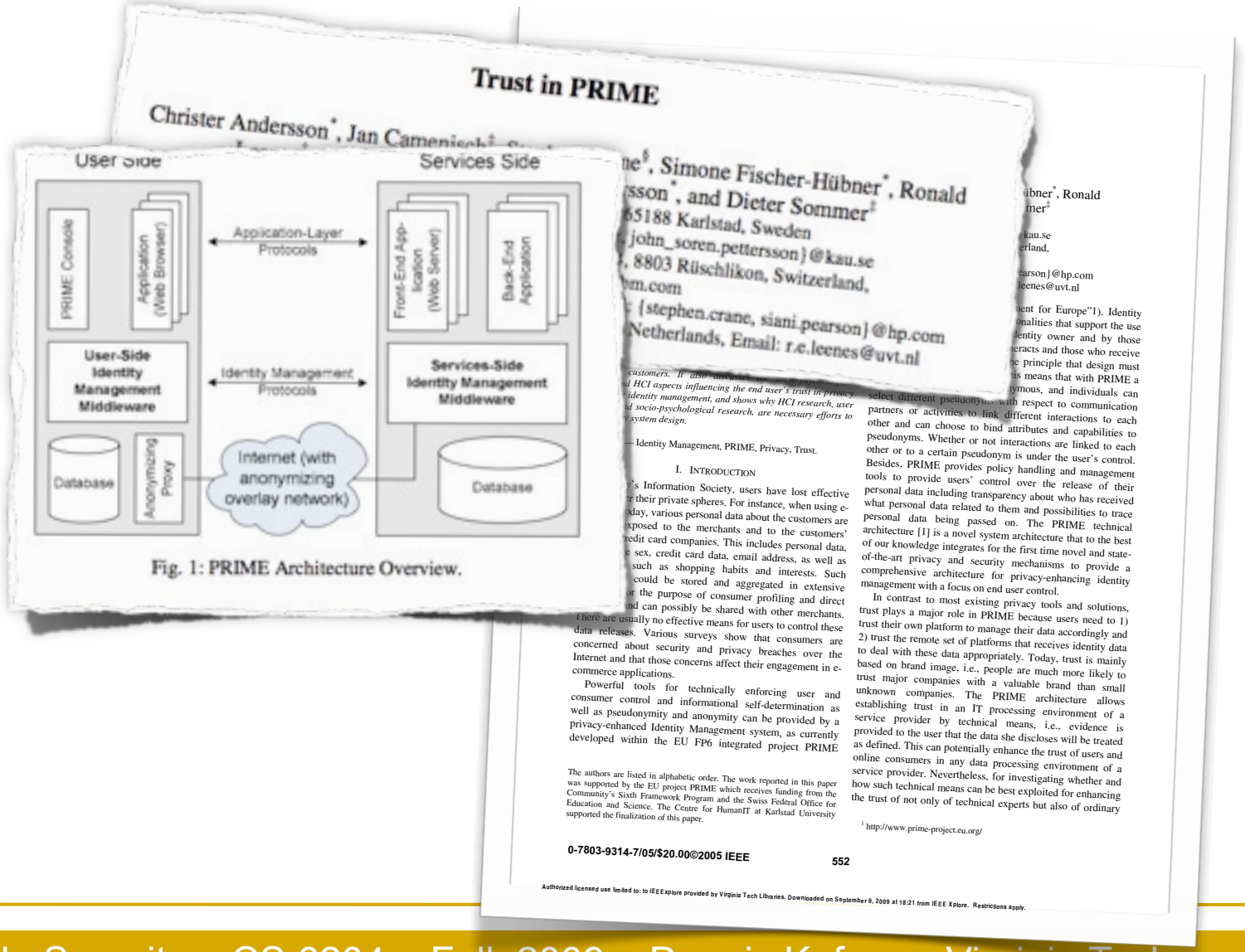
Revisiting PRIME

Stacy Branham

Remember PRIME?



Trust in PRIME

Christer Andersson*, Jan Camenisch‡ ... ne§, Simone Fischer-Hübner*, Ronald ... sson*, and Dieter Sommer‡ ... 65188 Karlstad, Sweden ... john_soren.pettersson}@kau.se ... , 8803 Rüschlikon, Switzerland, ... om.com ... {stephen.crane, siani.pearson}@hp.com ... Netherlands, Email: r.e.leenes@uvt.nl

User Side | Services Side

PRIME Console | Application (Web Browser) | Application-Layer Protocols | Front-End Application (Web Server) | Back-End Application

User-Side Identity Management Middleware | Identity Management Protocols | Services-Side Identity Management Middleware

Database | Anonymizing Proxy | Internet (with anonymizing overlay network) | Database

Fig. 1: PRIME Architecture Overview.

customers. It also discusses ... and HCI aspects influencing the end user's trust in privacy ... identity management, and shows why HCI research, user ... socio-psychological research, are necessary efforts to ... system design.

— Identity Management, PRIME, Privacy, Trust.

I. Introduction

... 's Information Society, users have lost effective ... their private spheres. For instance, when using e- ... oday, various personal data about the customers are ... xposed to the merchants and to the customers' ... redit card companies. This includes personal data, ... e sex, credit card data, email address, as well as ... such as shopping habits and interests. Such ... could be stored and aggregated in extensive ... or the purpose of consumer profiling and direct ... nd can possibly be shared with other merchants. There are usually no effective means for users to control these data releases. Various surveys show that consumers are concerned about security and privacy breaches over the Internet and that those concerns affect their engagement in e-commerce applications.

Powerful tools for technically enforcing user and consumer control and informational self-determination as well as pseudonymity and anonymity can be provided by a privacy-enhanced Identity Management system, as currently developed within the EU FP6 integrated project PRIME

The authors are listed in alphabetic order. The work reported in this paper was supported by the EU project PRIME which receives funding from the Community's Sixth Framework Program and the Swiss Federal Office for Education and Science. The Centre for HumanIT at Karlstad University supported the finalization of this paper.

0-7803-9314-7/05/$20.00©2005 IEEE

552

... ibner*, Ronald ... mer‡ ... kau.se ... erland, ... earson}@hp.com ... leenes@uvt.nl ... ent for Europe"1). Identity ... onalities that support the use ... dentity owner and by those ... eracts and those who receive ... e principle that design must ... us means that with PRIME a ... ymous, and individuals can select different pseudonyms with respect to communication partners or activities to link different interactions to each other and can choose to bind attributes and capabilities to pseudonyms. Whether or not interactions are linked to each other or to a certain pseudonym is under the user's control. Besides, PRIME provides policy handling and management tools to provide users' control over the release of their personal data including transparency about who has received what personal data related to them and possibilities to trace personal data being passed on. The PRIME technical architecture [1] is a novel system architecture that to the best of our knowledge integrates for the first time novel and state-of-the-art privacy and security mechanisms to provide a comprehensive architecture for privacy-enhancing identity management with a focus on end user control.

In contrast to most existing privacy tools and solutions, trust plays a major role in PRIME because users need to 1) trust their own platform to manage their data accordingly and 2) trust the remote set of platforms that receives identity data to deal with these data appropriately. Today, trust is mainly based on brand image, i.e., people are much more likely to trust major companies with a valuable brand than small unknown companies. The PRIME architecture allows establishing trust in an IT processing environment of a service provider by technical means, i.e., evidence is provided to the user that the data she discloses will be treated as defined. This can potentially enhance the trust of users and online consumers in any data processing environment of a service provider. Nevertheless, for investigating whether and how such technical means can be best exploited for enhancing the trust of not only of technical experts but also of ordinary

[1] http://www.prime-project.eu.org/

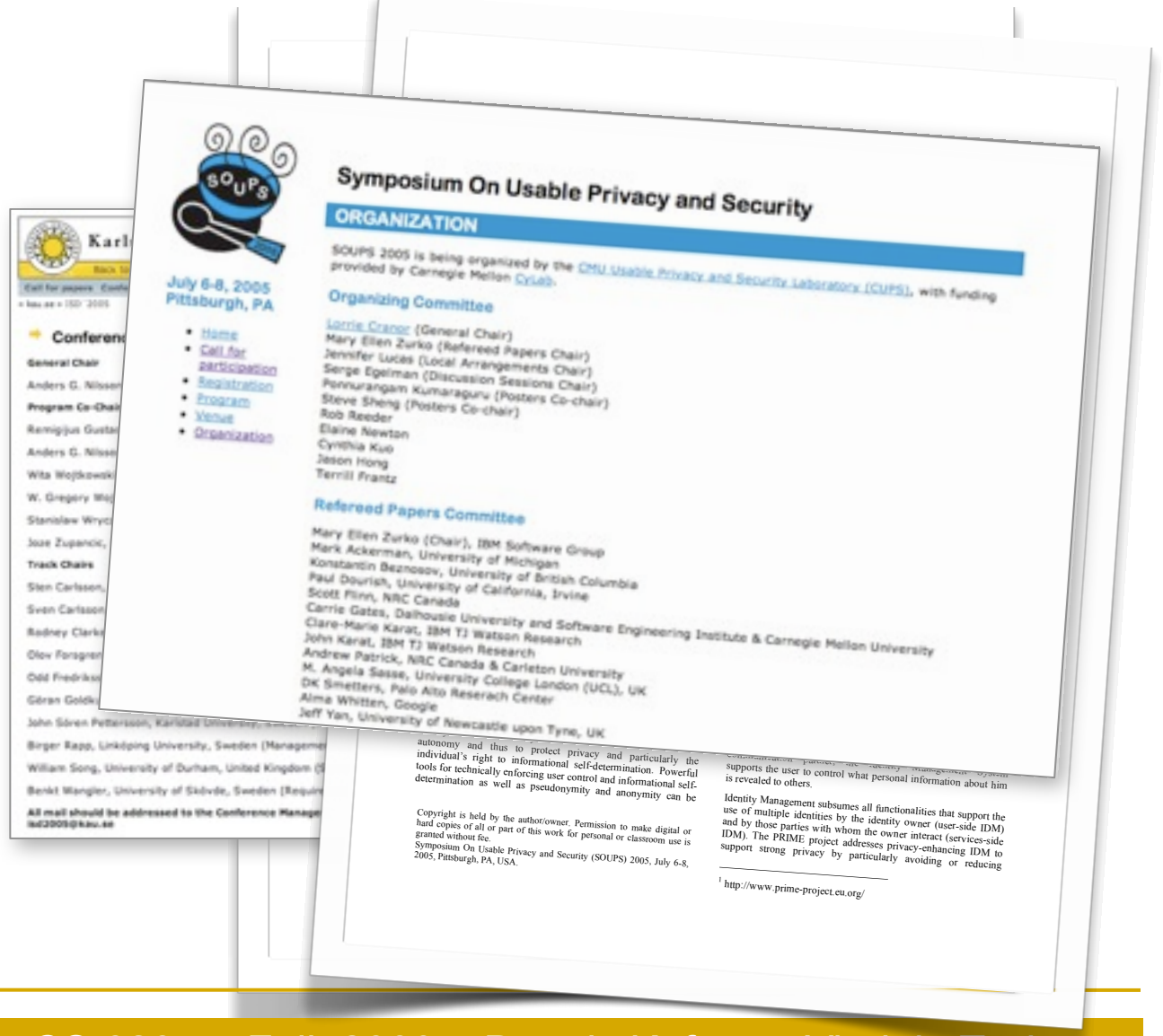
Outline

- Introduction
  - the Papers
  - the PRIME Project
- Summary & Critique of Bergmann et al.
- Summary & Critique of Pettersson et al.
- Discussion

Introduction: the Papers

Pettersson

Bergmann



Introduction: the PRIME project

Paper 1

- *Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology*

  Bergmann, Rost, Pettersson

- ISD 2005, 8 cites

Exploring the Feasibility of a Spatial User Interface Paradigm for Privacy-Enhancing Technology

Mike Bergmann[1], Martin Rost[2] and John Sören Pettersson[3]

[1] Technical University Dresden, Germany. mb41@inf.tu-dresden.de
[2] Independent Centre for Privacy Privacy Protection (ICPP), Germany. martin.rost@datenschutzzentrum.de
[3] Karlstad University, Sweden. john_soren.pettersson@kau.se

Introduction

Electronic devices get more and more involved in many of our communication processes for personal and professional activities. Each communication process may implicitly affect our privacy. An example may be the location trace of mobile phones. Experts present identity management systems to preserve the user's[1] privacy [2]. In digital correspondence users should decide about disclosure of personally identifiable information (in the following simply called "data"). However, identity management for Everyman is not yet a commonplace.

To address the whole area of identity management, it is necessary to find an easy to understand model similar to the usage of a phone or a debit card. We suppose that after the shell and command line solutions and the window-based interface, one now has to look for a new paradigm to provide more intuitive handling of the communication process and work flow.

In particular, we have been interested in how to facilitate for users to manage several preference settings, so that different communication partners are treated differently by the user's identity management tool without demanding the user to change settings during ordinary use of his communication devices. We refine the "Virtual City" idea, originally proposed by Andreas Pfitzmann and published in [7], using a town map as a user interface, to manage identity related processes regarding these devices. This interface could potentially allow users with various levels of education to manage their digital identities intuitively by transferring their existing ex-

[1] In the context of this paper, the term "user" describes the person who is using the digital equipment related to the identity management sensitive activities.

Advances in Information Systems Development: Bridging the Gap between Academia and Industry. Edited by A.G. Nilsson et al., Springer, 2005

Motivation/Overview

- electronic devices facilitate communication
  - hence, pose privacy & security risks
- users should control personal info disclosure (identity mgmt, info self-determination)
  - preference settings management
  - diff roles, diff communicators treated differently
  - not required to change settings in ordinary use
  - for users of various levels of education
- new paradigm, spatial interface, “Virtual City”
- study of PRIME UI

The TownMap

- "hierarchical"
- richness of possible structure
- intuitive
- each space corresponds to a bundle of prefs.
- set several prefs. at once

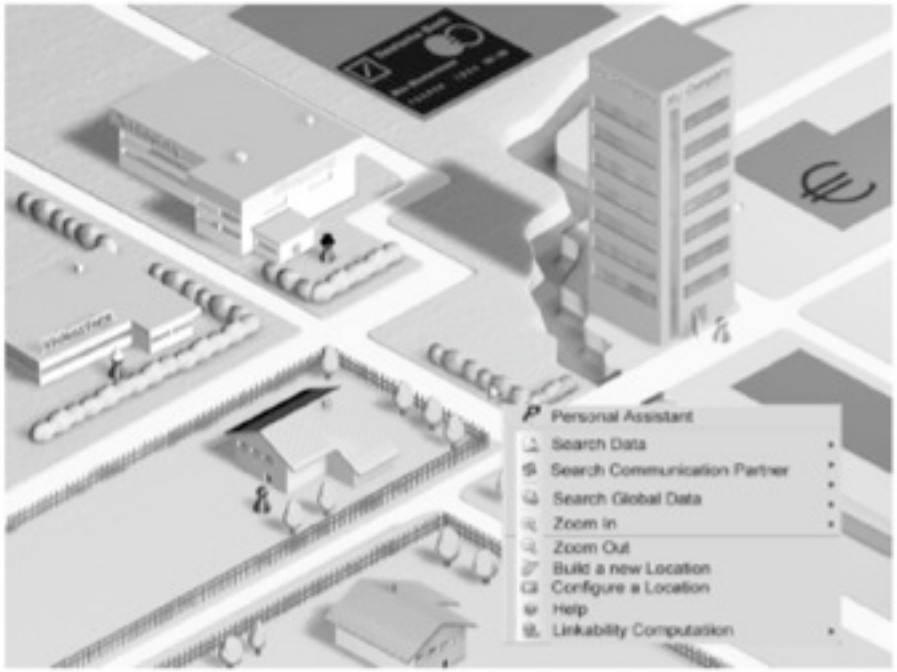


Fig. 1. A town map with some attributes and a simple drop-down menu

The Town Map, Cont'd

- different regions
  - bounded by "districts," "walls," "connectors"
  - objects arranged by "similarity"
  - predefined policy with at least 4 areas
    - public area = anonymous
    - business related area = employer knows more
    - my home area (inside private area) = personal
    - private area = specific close contacts have access
- entering new area will change privacy settings to those defined for that area

User Study

- 34 undergraduates
- Lecture hall batches
- Pictures and animated narrative shown
- Use Cases:
  - opening up communication with a SP
  - user connected to two SP's
  - user connects to an unfamiliar SP
- 2 interfaces: 3D TownMap & 2D CrossRoad
  - TownMap was populated with more objects than the browser

User Study

- Comparative study
- Scenario
- Questionnaire?

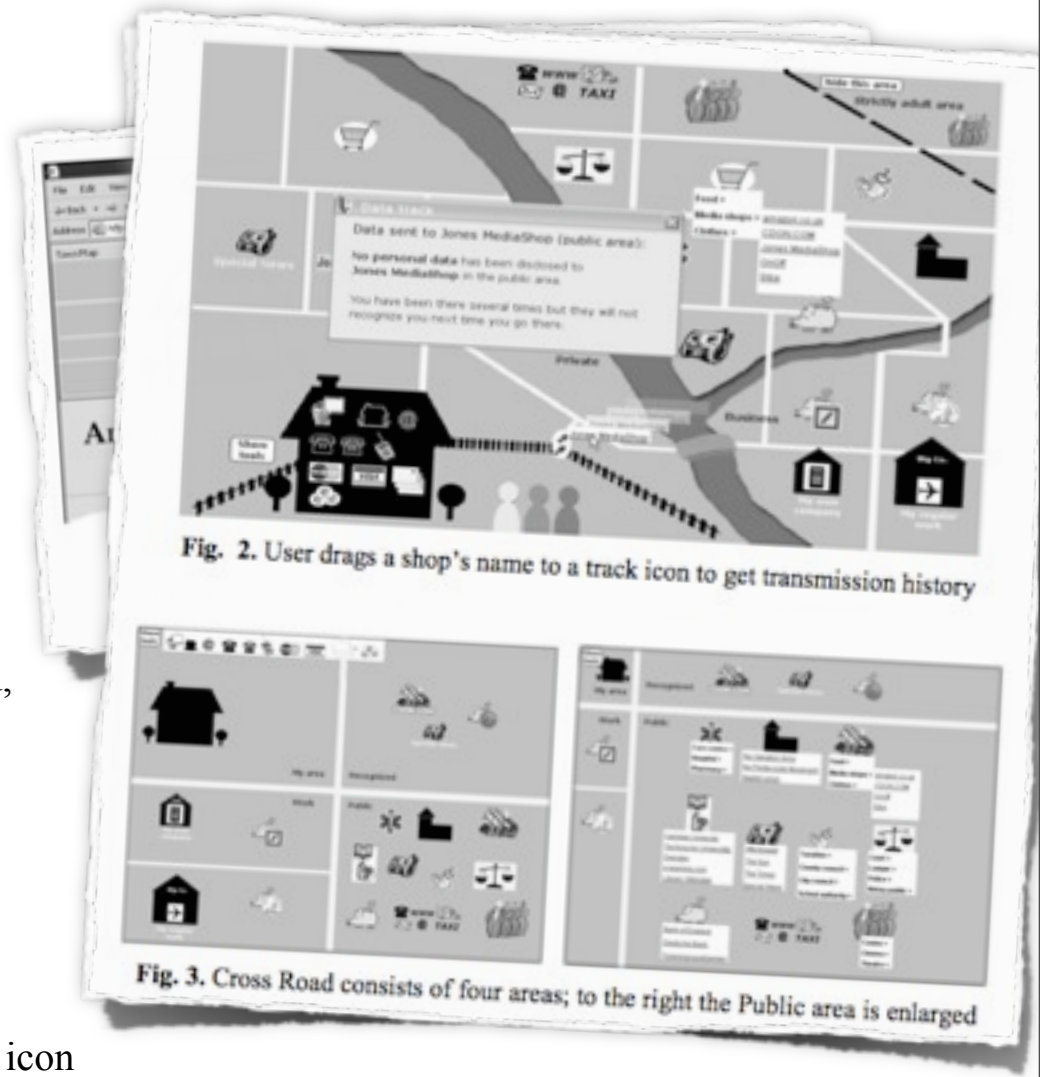


Fig. 2. User drags a shop's name to a track icon to get transmission history

Fig. 3. Cross Road consists of four areas; to the right the Public area is enlarged

"...the goal was not to see if a town map was better than a traditionally styled browser. Instead, the purpose was to get a basis for discussions within the PRIME project, and of course with interested parties in the rest of the research community, about the semiotic dimension one should venture to play on in more costly prototyping."

"The user dragged a name icon and a credit card icon to a pay service; his own house and two icons representing the relevant service providers were visible in a tilted town map shown in Figure 4. Later the user also inquired about who had received his name by dropping his name icon on a symbol for his data transactions database (Figure 2)."

Results

"As expected, the traditional-styled browser got in general a positive response. More than half of the answers gave positive descriptions of it. The maps, on the other hand, were considered by many to be messy."

"On the question about their impression of the display of data and money transaction, 19 answered that it facilitates while 11 regarded it as superfluous. Nine of these eleven persons also thought that it looked childish; fifteen thought it looked OK."

"When ranking the alternatives, 24 persons put the traditional browser as their primary choice; they also seemed to prefer the simple CrossRoad as a secondary choice. Seven preferred the realistic TownMap and three preferred the simplified CrossRoad, but there was no tendency for the secondary choice."

"Two fifths of the participants answered that they would like to be able to switch between designs."

"One should further note that more than half of the participants answered that animation of transactions 'facilitates.'"

-Bergmann et al., 2005

Discussion

- there was “some interest” in the town map
- maps may have seemed messier because more objects were in the town map
- meaningful to use TownMap-like formats for informing the user of ongoing transactions or for getting user input on data releases

“...the question of visualizing with a town map may not only be thought of as replacing the old desktop but may be introduced via the back door of tutorials.” *-Bergmann et al., 2005*

Criticism

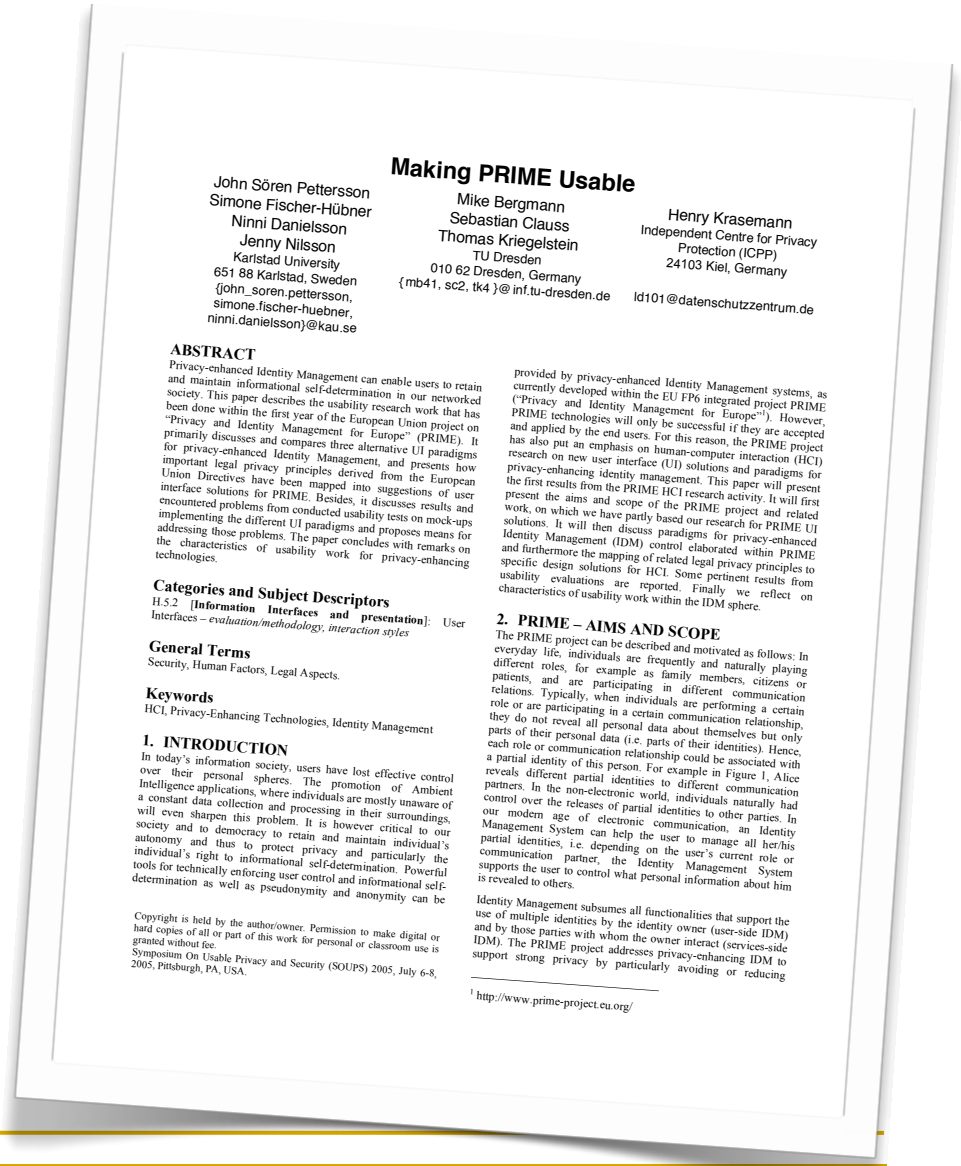
- unclear description of the system
- poor study design for the conclusions
- weak/unsubstantiated results

Paper 2

- *Making Prime Usable*

  Pettersson, Hübner, Danielsson, Nilsson, Bergmann, Clauss, Kriegelstein, Krasemann

- SOUPS 2005, 16 cites



Making PRIME Usable

John Sören Pettersson
Simone Fischer-Hübner
Ninni Danielsson
Jenny Nilsson
Karlstad University
651 88 Karlstad, Sweden
{john_soren.pettersson, simone.fischer-huebner, ninni.danielsson}@kau.se

Mike Bergmann
Sebastian Clauss
Thomas Kriegelstein
TU Dresden
010 62 Dresden, Germany
{mb41, sc2, tk4 }@ inf.tu-dresden.de

Henry Krasemann
Independent Centre for Privacy Protection (ICPP)
24103 Kiel, Germany
ld101@datenschutzzentrum.de

ABSTRACT

Privacy-enhanced Identity Management can enable users to retain and maintain informational self-determination in our networked society. This paper describes the usability research work that has been done within the first year of the European Union project on "Privacy and Identity Management for Europe" (PRIME). It primarily discusses and compares three alternative UI paradigms for privacy-enhanced Identity Management, and presents how important legal privacy principles derived from the European Union Directives have been mapped into suggestions of user interface solutions for PRIME. Besides, it discusses results and encountered problems from conducted usability tests on mock-ups implementing the different UI paradigms and proposes means for addressing those problems. The paper concludes with remarks on the characteristics of usability work for privacy-enhancing technologies.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and presentation**]: User Interfaces – *evaluation/methodology, interaction styles*

General Terms

Security, Human Factors, Legal Aspects.

Keywords

HCI, Privacy-Enhancing Technologies, Identity Management

1. INTRODUCTION

In today's information society, users have lost effective control over their personal spheres. The promotion of Ambient Intelligence applications, where individuals are mostly unaware of a constant data collection and processing in their surroundings, will even sharpen this problem. It is however critical to our society and to democracy to retain and maintain individual's autonomy and thus to protect privacy and particularly the individual's right to informational self-determination. Powerful tools for technically enforcing user control and informational self-determination as well as pseudonymity and anonymity can be provided by privacy-enhanced Identity Management systems, as currently developed within the EU FP6 integrated project PRIME ("Privacy and Identity Management for Europe"[1]). However, PRIME technologies will only be successful if they are accepted and applied by the end users. For this reason, the PRIME project has also put an emphasis on human-computer interaction (HCI) research on new user interface (UI) solutions and paradigms for privacy-enhancing identity management. This paper will present the first results from the PRIME HCI research activity. It will first present the aims and scope of the PRIME project and related work, on which we have partly based our research for PRIME UI solutions. It will then discuss paradigms for privacy-enhanced Identity Management (IDM) control elaborated within PRIME and furthermore the mapping of related legal privacy principles to specific design solutions for HCI. Some pertinent results from usability evaluations are reported. Finally we reflect on characteristics of usability work within the IDM sphere.

2. PRIME – AIMS AND SCOPE

The PRIME project can be described and motivated as follows: In everyday life, individuals are frequently and naturally playing different roles, for example as family members, citizens or patients, and are participating in different communication relations. Typically, when individuals are performing a certain role or are participating in a certain communication relationship, they do not reveal all personal data about themselves but only parts of their personal data (i.e. parts of their identities). Hence, each role or communication relationship could be associated with a partial identity of this person. For example in Figure 1, Alice reveals different partial identities to different communication partners. In the non-electronic world, individuals naturally had control over the releases of partial identities to other parties. In our modern age of electronic communication, an Identity Management System can help the user to manage all her/his partial identities, i.e. depending on the user's current role or communication partner, the Identity Management System supports the user to control what personal information about him is revealed to others.

Identity Management subsumes all functionalities that support the use of multiple identities by the identity owner (user-side IDM) and by those parties with whom the owner interact (services-side IDM). The PRIME project addresses privacy-enhancing IDM to support strong privacy by particularly avoiding or reducing

[1] http://www.prime-project.eu.org/

Motivation/Overview

- Users have lost control of personal info
- Ambient intelligence apps exacerbate this
- Critical to democracy to maintain autonomy and right to *information self-determination*
- PRIME is an Identity Management (IDM) system that addresses this need
- Three design paradigms for IDM PRIME
- Legal requirements inform PRIME usability
- HCI studies of PRIME IDM paradigms

PRIME

- roles, partial identities
- user/services-side IDM
- design must start from max privacy
- user-controlled pseudonyms
- user-controlled linkability

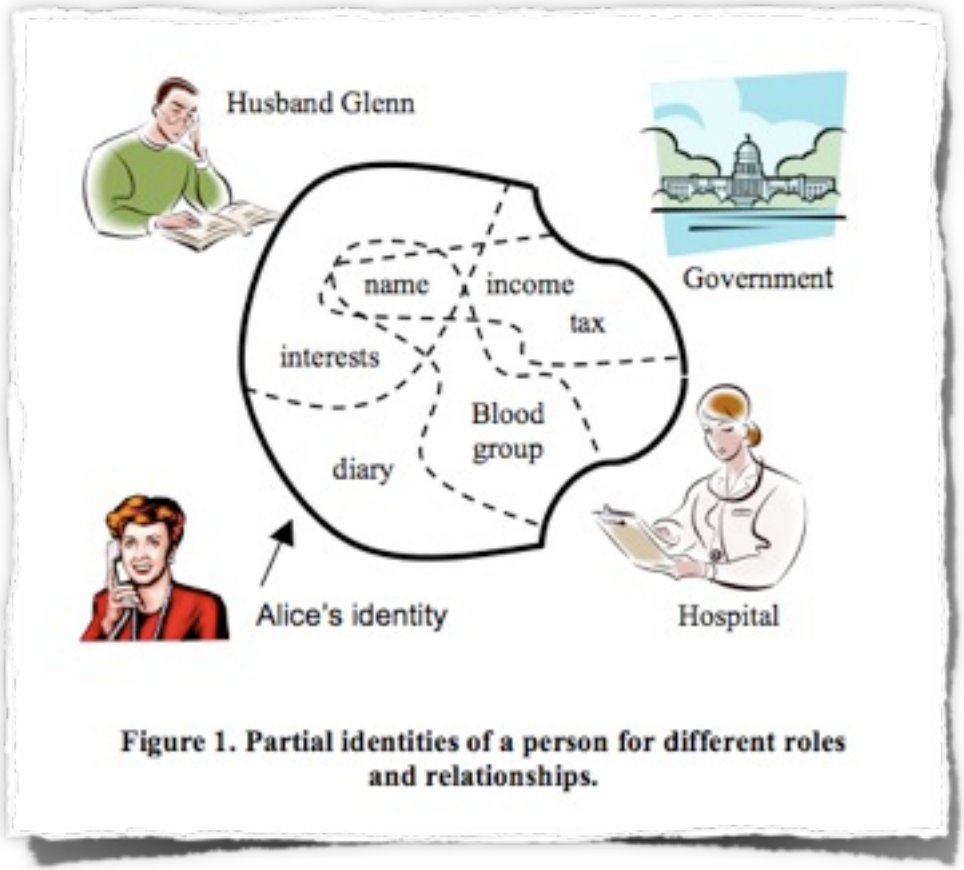


Figure 1. Partial identities of a person for different roles and relationships.

PISA

- derived HCI guidelines from privacy law
- Just-In-Time-Click-Through Agreements (JITCTAs)
- Drag-And-Drop Agreements (DADAs)
- PRIME seeks to build off PISA

Role-centered Paradigm

- control of data dictated by roles
- each role has different disclosure prefs. for diff. data types
- icon bar that fits into browser
- user has to click role before transaction, has to switch role when is no longer appropriate
- didn't user test these mockups

Relationship-centered Paradigm

- user defines diff. privacy prefs. for each service provider
- bookmarks are used to store service providers
  - default relationship is “anonymous” but can be overridden
- no extra steps introduced during browsing

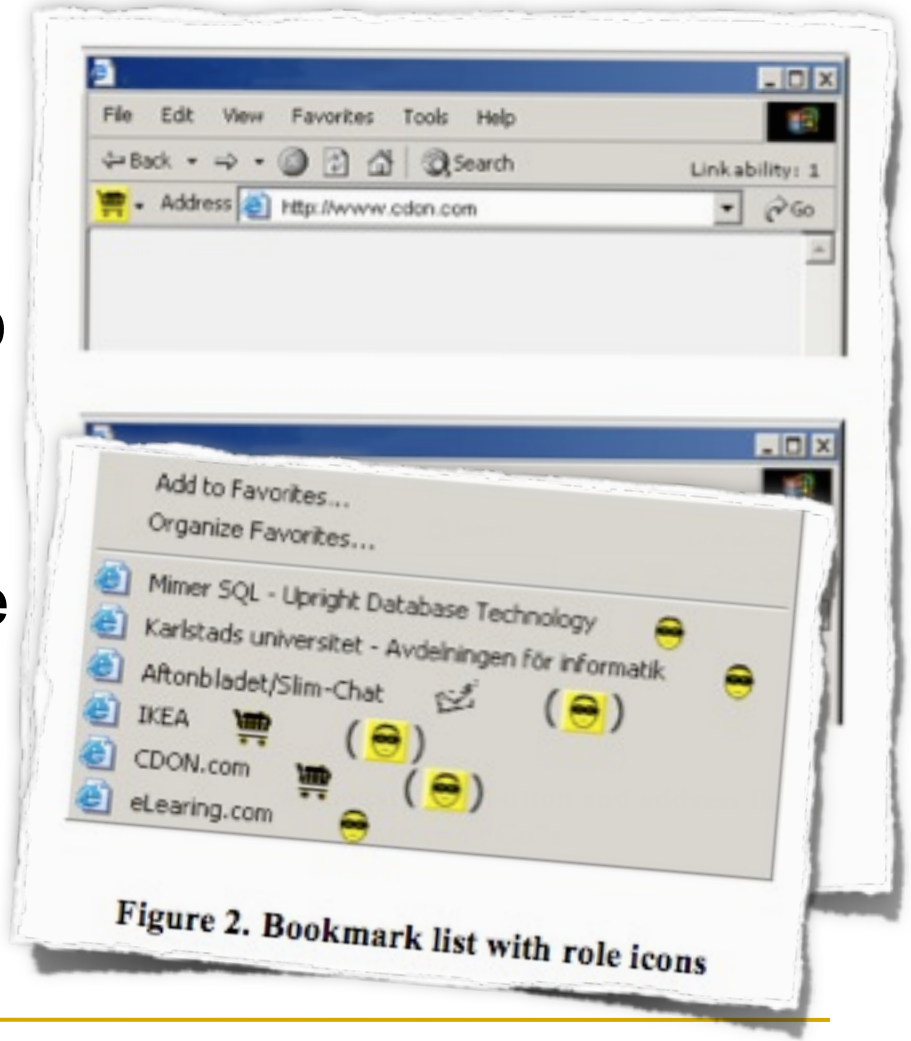


Figure 2. Bookmark list with role icons

TownMap-based Paradigm

- roles map to areas
  - Neighborhood (rel. pseudonymity, default)
  - Public (trans. pseudonymity, default)
  - Work (rel., role pseudonymity)
- houses
  - user's house
  - bookmarked service providers

Figure 4. TownMap with building tools visible

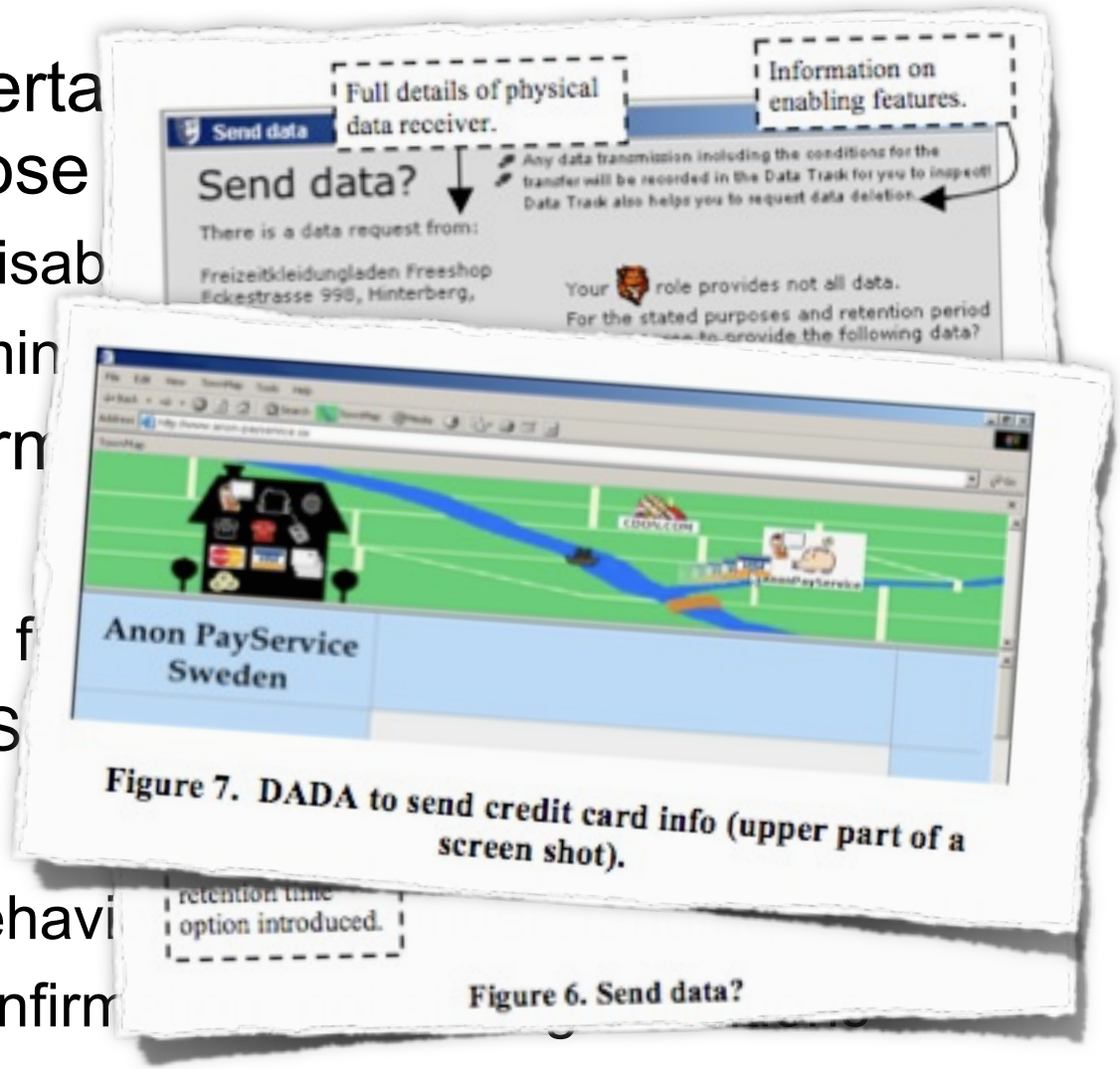
Figure 5. Tilted TownMap visible

Legal Privacy Requirements to PRIME

Legal policy	Info to be provided to user	user right to access / rectify / block / erase data & object	obtaining consent from user	data minimization
PISA HCI Guidelines	users must know who is controlling data and for what purpose	user is conscious of, understand, and can exercise rights	“unambiguous,” “explicit,” or “informed” user consent	n/a
PRIME HCI Guidelines	machine-readable policy, displayed by PRIME UI, link to full policy,	info about data subject’s rights has to appear in the policy, obvious tools for exercising rights	automatic disclosure; dialogue box; mobile phone informed consent; consent by DnD	possible conflict: predefined roles and defaults

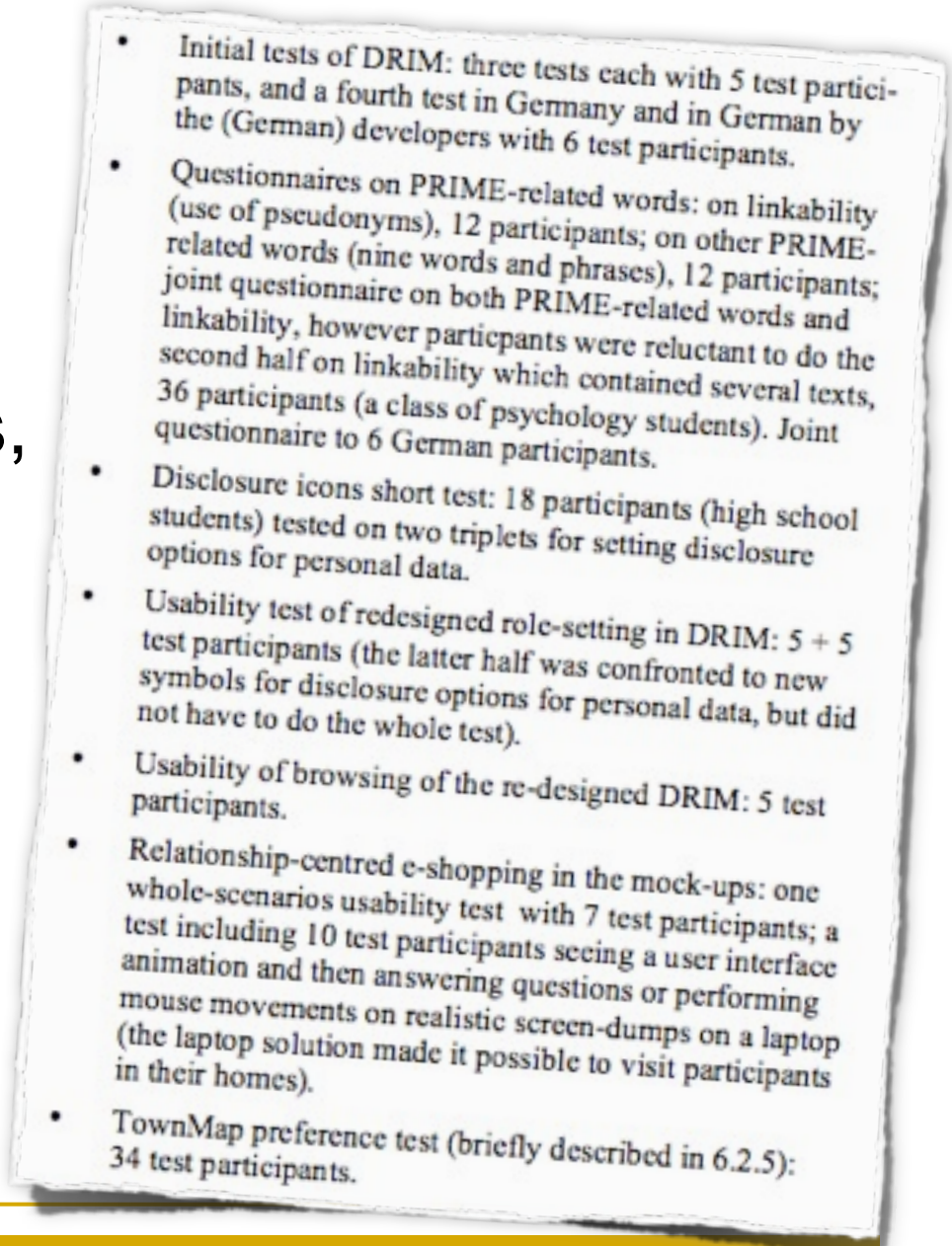
Obtaining User Consent

- auto disclosure: certa
  for specified purpose
  - user can change/disab
  - user should be remin
- dialogue box: inform
- mobile phone IC
  - linked or scrollable f
  - bandwidth limits, "S
- consent by DnD
  - avoid automatic behavi
  - can be used for confirm



Evaluation

- 8 usability tests, 71 participants
- 2 sets questionnaires, 34 participants
- 1 comparison, 66 participants
- pilots, interactive mockups, 1-on-1 post-interviews



- Initial tests of DRIM: three tests each with 5 test participants, and a fourth test in Germany and in German by the (German) developers with 6 test participants.
- Questionnaires on PRIME-related words: on linkability (use of pseudonyms), 12 participants; on other PRIME-related words (nine words and phrases), 12 participants; joint questionnaire on both PRIME-related words and linkability, however participants were reluctant to do the second half on linkability which contained several texts, 36 participants (a class of psychology students). Joint questionnaire to 6 German participants.
- Disclosure icons short test: 18 participants (high school students) tested on two triplets for setting disclosure options for personal data.
- Usability test of redesigned role-setting in DRIM: 5 + 5 test participants (the latter half was confronted to new symbols for disclosure options for personal data, but did not have to do the whole test).
- Usability of browsing of the re-designed DRIM: 5 test participants.
- Relationship-centred e-shopping in the mock-ups: one whole-scenarios usability test with 7 test participants; a test including 10 test participants seeing a user interface animation and then answering questions or performing mouse movements on realistic screen-dumps on a laptop (the laptop solution made it possible to visit participants in their homes).
- TownMap preference test (briefly described in 6.2.5): 34 test participants.

Discussion

- users had diverse preferences for icons to symbolize roles
  - so, let users define icon
- users had problem me
  and services-side IDM
  - HCI principle: UI should
- users have trouble tru
  although reasoning is
  - visible assurances that
- unclear perception of i
  pseudonyms and "real
  - prevent manual entry of
- transaction animations

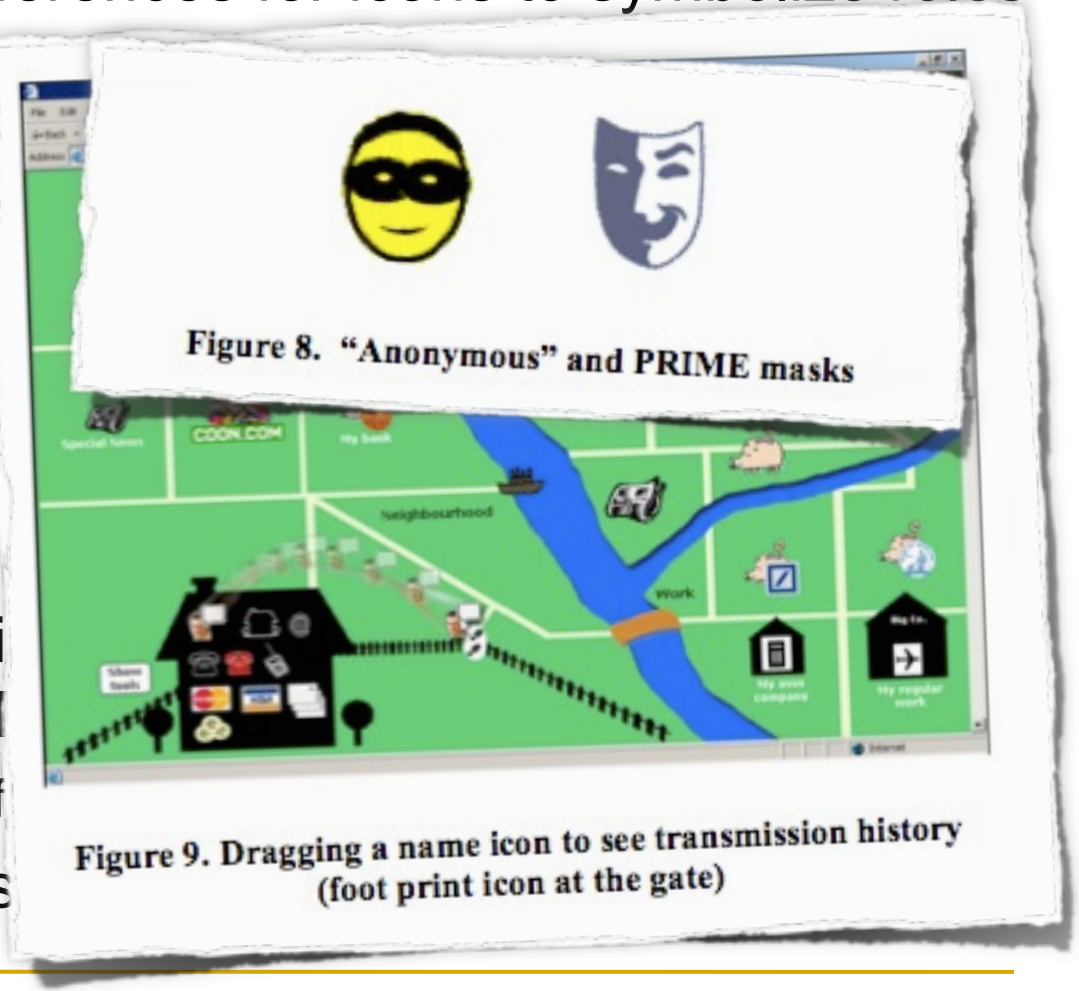


Figure 8. "Anonymous" and PRIME masks

Figure 9. Dragging a name icon to see transmission history (foot print icon at the gate)

Criticism

- contributions
  - 3 paradigms
  - law-derived PRIME usability guidelines
- study findings are weakest
  - not enough methodological description
  - not enough raw data presented

Class Discussion

- informational self-determination?

Dan Ariely, "Are We In Control of Our Own Decisions?" 2008 TED Talk

- what does this mean for us? research? ethics?

Class Discussion

"'Int
info
app
afte

Current Research

Supporting Trust Decisions

See older projects here...

Internet users are increasingly being asked to make trust decisions, and the consequences of a wrong decision can lead to viruses, spyware, and identity theft. Our goal is to understand how people make trust decisions, currently in the context of phishing scams, and to develop user interfaces, algorithms, and other support tools to help people make better decisions. This work is funded by National Science Foundation CCF-0524189

- Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer (APWG eCrime 2007)
- User Interfaces and Algorithms for Fighting Phishing, a talk in August 2007 summarizing our work to date. An older version of this talk is available as a Google TechTalk.
- Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish (SOUPS2007)
- Anti-Phishing Phil game
- CANTINA: A Content-Based Approach to Detecting Phishing Web Sites (WWW2007)
- Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System (CHI 2007)
- Phinding Phish: An Evaluation of Anti-Phishing Toolbars (NDSS 2007)

- Does education have a role?

Class Discussion

- Is TownMap *a priori* better than a slider bar?

TownMap	Slider Bar
- difficult metaphor	+ standard metaphor
+ may increase awareness of how many institutions have their information	+ probably faster
<add your own>	<add your own>

Class Discussion

- how do we know that we can trust these user studies if we are missing methodology, results in the papers?

"I believe that all research ultimately depends on trust, whether it is qualitative or quantitative" *-Deborah Tatar, in a meeting 11/18/09*

- What counts as evidence?
- What counts as substantial contribution?

“As Allan Cooper explained about targeting a product to a receptive user group: “80% of people in focus groups hated the new Dodge Ram pickup. [Chrysler] went ahead with production, and made it into a bestseller because the other 20% loved it. Having people love your product, even if it is only a minority, is how you succeed.” *-Bergmann et al., 2005*

Goals/Values

- important to limit up-front customization while providing for variety of customization
- should help the user enforce his rights of informational self-determinism
- should avoid PET jargon
- should be “comfortable” for both novice & expert users
- should not require explicit learning process
- should not demand extra clicks/key-presses
- should err on the side of anonymity