PRIME – Privacy and Identity Management for Europe

Identity Management for eCustomers

Data traces everywhere?

Which data do customers leave during an ordinary e-shopping session and who will have access to this data? Naturally customers disclose some kind of payment information to the shop (service provider) as well as their shipping address when goods have to be delivered. However, users involuntarily leave many additional data traces. In a classical e-shopping scenario, data about the customer's shopping habits and interests are exposed at the merchant's and payment institute's sides. Utilising cookies, the service provider is able to identify users at their next visit and can display offers matching their interests recorded during previous sessions. Placing ads on different web sites, it becomes possible to track and profile users beyond the scope of the own web site. Thus customers usually leave more data than necessary when shopping online. Once the user provides his personal data during the ordering process, all the collected data traces can be linked to the disclosed personal information. Storing this information, the service provider is able to further profile their customers.

Consequences may include an increase of spam, personalised ads and commercial telephone calls. Depending on the privacy policy of the provider the customer may even have unknowingly "consented" to the circulation of his data. Even worse is the threat of identity theft. Having harvested and linked enough data about a person, it gets easy to impersonate the user with fraudulent ambition – either harming the user or third persons. For example bidding on ebay under a "stolen" identity may ruin the customer's online reputation, using another person's credit card information to pay for premium content will do financial harm.

This Primer introduces the concept of identity management, policies and transparency. Emerging tools enabling customers to apply user-centric identity management are described – they provide a sophisticated countermeasure against identity theft and user tracking. Finally this Primer points to currently available reliefs to protect one's privacy as a customer.

Identity Management

A solution to these threats is offered by user-centric identity management (IdM). In the offline world we intuitively disclose only the relevant information to our communication partners. This way the employer will know information about one's education and salary, while friends will rather have knowledge about hobbies, nicknames and personal preferences [see Fig. 1]. The equivalent oft partial identities in the online world is the use of different login names on different websites and during different shopping sessions at the same site. Modern identity management systems are a toolbox offering possibilities to create, manage, employ and delete different identities. The key issues of user-controlled IdM are to empower the user and to increase transparency.

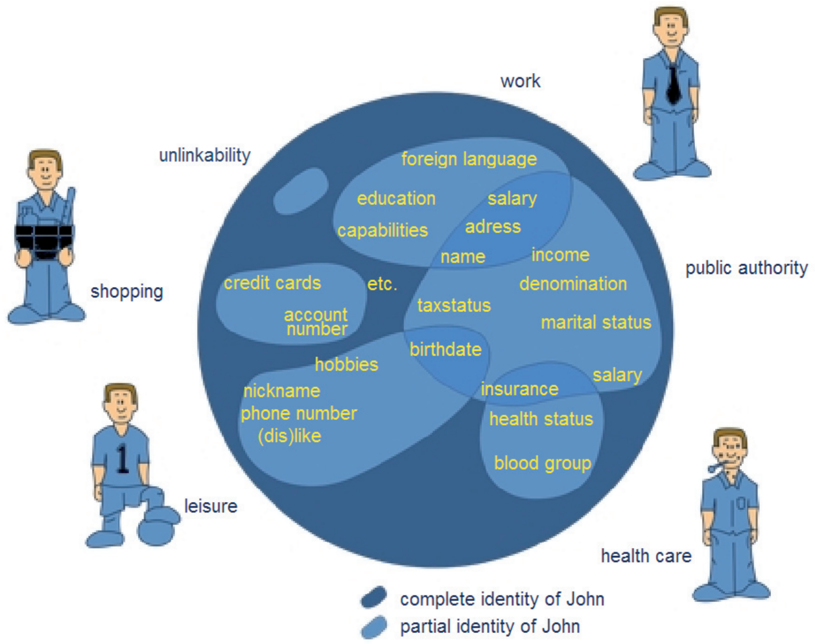

Figure 1: Partial Identities

User-centric approach & transparency

In a future step user-controlled identity management system could enable the user to control his personal data by defining policies. A policy is a guideline concerning disclosure, use and manipulation of data, especially user-specific personal data. A privacy policy is as special policy, where the service provider stipulates for which purposes and to what extent he collects, stores or transfers data after the transaction has finished. In principle such policies can be applied by customers and service providers alike.

At present policies of service providers are usually drafted as legal texts – barely understandable and hardly read by customers. Therefore users often do not know what happens with their data. However, transparency should be a concern for vendors as it affects the customers' trust and loyalty towards the service provider.

The requirement of transparency is also laid out in the European Data Protection Directive requiring that the user has to be informed in an understandable manner by the processing party about any intended use of personal data exceeding the necessary usage for the fulfilment of the contract. One solution to achieve understandable policies is the "layered policies approach" as recommended by the Article 29 Working Party [1]. The working party suggests that the full privacy policy should be prefixed with a short and a condensed notice outlining the essentials and offering a click-through to more detailed explanations of the full policy.

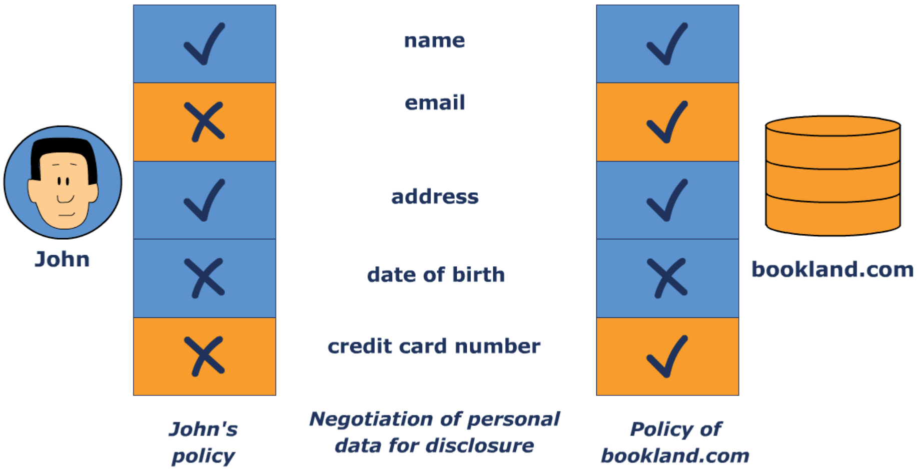

Figure 2: Policy Managemement

In the future machine readable policies will allow an automated comparison of privacy policies with preferences set by the consumer and inform him about relevant aberrations [see Fig. 2]. For example a user named John defined within his policy that he does not want to provide his e-mail address and credit card information. Before conveniently filling the web form, the software warns John that the bookland.com store nevertheless requires these data and enables John to either consent to the data transfer, to quit the transaction or, provided that the shop enables that feature on the server side, to negotiate about the data that must be provided. PRIME partners are involved in standardising protocols for the exchange of machine readable policies.

Enforcing policies by technology

Carrying on the idea of user defined privacy policies, disclosed information may be tagged with so called "sticky policies". The user's policy will be cryptographically associated with the information functioning as gate keeper to the data. Even though it cannot be guaranteed that the service provider will adhere to the binding between the collection's purpose and the data's actual uses, data abuse will get less likely.

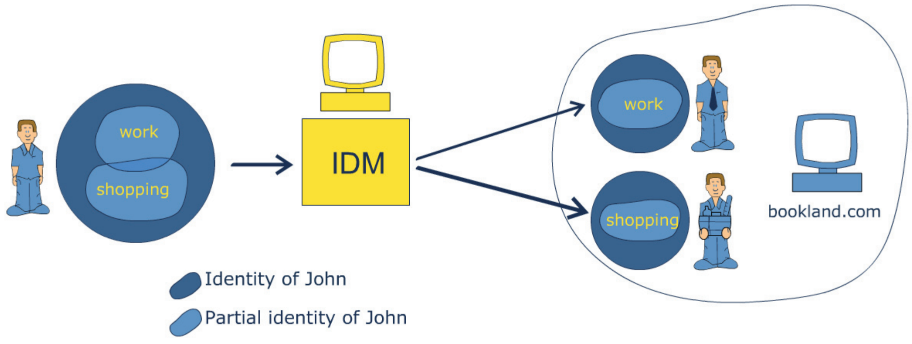

Figure 3: Handling of partial identities

Another approach is based on the fact that it is not necessary that all involved partners get access to all information. Supposed the store has outsourced the delivery to a logistic provider. Then the logistic partner will need the name and shipping address but not the payment information needed for the credit card processor. In a future scenario the service provider does not need to receive any personal information about the customer. Instead the user provides a so called credential. Based on cryptographic methods, a trusted third party issues a credential telling the store that the customer has provided a valid shipping address which will be disclosed to the logistic partner. Anonymous payment will possible with e-coins, a serial number signed by a bank. This way the shop will not get any access to the customer's data unless it must be disclosed by the third party, i.e., in case of fraudulent behaviour of the customer.

Enforcing privacy today: using alias names

So what can be done to protect one's privacy until identity management solutions are widely available?

To be on the safe side, users should disclose as little personal data as possible. Using different aliases whenever feasible makes it harder to link data traces. Only the information necessary for the performance of the contract should be provided, e.g., if a contract about the delivery of goods is conducted, an e-mail address usually can not be deemed necessary. If the website nevertheless requires this information, a disposable e-mail address may be provided. If the user decides to provide fake data, no harm may be done to the contract partner or anyone else. In particular name, address and payment information must be correct. For some contracts special laws require further data collection, e.g., banks have to collect personal data due to legislation on the prevention of money laundering. In this case all required information must be correctly provided.

Customers are also supported by some readily available software solutions for identity management, which provide in their basic functionality tools for the administration of partial identities assisting the user in handling the plurality of accounts and passwords [see Fig 3]. Advanced functions include convenient form filling functions and a history management that allows reviewing which partial identity has been used and which data provided to whom. The EU-funded project PrimeLife plans to develop and release a fully functional software solution for identity management with the mentioned functionalities [www.primelife.eu].

Other easily implementable solutions include the use of encryption during online sessions to prevent access of third parties to the transferred data. Whether the current connection is secure is displayed by a closed lock and by an URL beginning with "https://". Further the browser settings in regard to cookies should not allow a transmission to third parties web sites. To keep the surfing habits untraceable for third parties, anonymization software such as OnionCoffee developed by the PRIME project may be applied [www.prime-project.eu/prime_products/opensource/].

Disputes with service providers regarding privacy issues, in particular when service providers violate the customers right to privacy, can be addressed to the corporate data protection officer of the respective service provider. Should the service provider fail to respond within a reasonable time (two months), the member state's data protection commissioner in charge may be addressed for further assistance.

Further reading

Further information for eCustomers are provided within the PRIME White Paper and the PRIME General Public Tutorial (in several European languages). Both are available at the project's web site.

www.prime-project.eu/tutorials/

www.prime-project.eu/prime_products/whitepaper/

[1] Art.29WP100ofNov25,2004,11987/04/EN, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2004_en.htm

At a Glance

Project Reference:

IST-507591

PRIME's Objective:

Development of a working prototype of a privacy enhancing Identity Management System and demonstration of novel solutions for managing identities.

Project Duration:

March 2004-May 2008

Partners:

20 partners from industry, academia, research centres and data protection authorities

Costs:

About € 15,5 Million

Funding:

The PRIME project receives research funding from the European Union's Sixth Framework Programme and the Swiss Federal Office for Education and Science.

Contact:

Marit Hansen
t: +49-431-988-1214
f: +49-431-988-1223
prime@datenschutzzentrum.de

Date of publication of this Primer:

May 2008

Want More Info?

The PRIME movie, tutorials, White Paper and various deliverables are available online:
www.prime-project.eu