Extended Abstract

Enforcement of Individual Privacy Policies for Users of Communication Service Providers plus a Challenge in Online Privacy

Michael Marhoefer michael.marhoefer@nsn.com
Robert Seidl robert.seidl@nsn.com
Nokia Siemens Networks Gmbh & Co. KG, St.-Martin-Str. 53, D-81699 Munich, GERMANY

Executive Summary

This talk has two parts:

1. *Report on adding Individual Privacy Policies to NSN's Research Prototype for Identity Management (IDM)*

2. *Challenge for Research in Access/Usage Control:*
   "How to control in Web 2.0 the flow of PII bypassing today's IDM"

Introduction

For the purpose of this talk, we use a few informal definitions:

- **Communication Service Provider** (**CSP**): provider of communication services, e.g. mobile operator, ISP, fixed-line operator
- **Identity**: a set of Personally Identifiable Information (**PII**)
- **User-centric Identity Management** (**UCIDM**): User-controlled management of Identity information for this user's online interaction with all kinds of Service Providers (incl. CSPs, Internet Service Providers, Application Service Providers, Content Providers)

Nokia Siemens Networks (NSN) is a leading provider of large-scale solutions for Subscriber Data Management and Identity Management for CSPs. CSPs, similar to other Internet access providers are well-positioned to provide UCIDM services to their users. As CSPs provide their services for a fee, they do not dependent on monetizing personal data of their users. This is especially true in comparison with providers of "free" services in Web 2.0.

Part 1: Report on adding Individual Privacy Policies to NSN's Research Prototype for IDM

The first part of this talk reports some intermediate results of NSN's IDM Research team. According to the European principle of *informational self-determination*, our aim is to let the user control his/her identity information. As a result of conceptual research performed in 2009, our IDM research team is currently adding a new privacy policy process with a series of functions to NSN's IDM Research Prototype:

Dagstuhl Seminar Proceedings 10141
Distributed Usage Control
http://drops.dagstuhl.de/opus/volltexte/2010/2715

1) User registers his Identity with the CSP's Identity Provider
2) User sets his/her individual Privacy Policy by using an intuitive, relatively simple user interface for policy settings (to be optimized)
3) IdP is transforming the user settings into executable code
4) When a Relying Party is requesting a user ID, then the IdP will reply according to the respective Individual Privacy Policy
5) Finally, this may results in a gradual disclosure of the user's ID to a certain Relying Party according the user's individual privacy policy.

We foresee two different flavours for the UI (user interface), one for standard users and one for expert users. While standard users can just set their preferred level of privacy, expert users are able to express their preferences per ID attribute, (group of) relying party, and even to override policy decisions as exception of their policies. So far, we did not yet implement substantial policy negotiations between the service provider and the IdP (see standards like P3P, Kantara UMA). Please see slides 7 – 9 for initial considerations regarding the introduction of Levels of Privacy.

There are essentially two limits for the complexity of these privacy preferences and policies. One is the average user's limited awareness of privacy; the other is the requirement that IdP systems have to scale for up to some 100 million users per CSP.

Part 2: Challenge for Research in Access/Usage Control: "How to control in Web 2.0 the flow of PII bypassing today's IDM"

While for Closed Infrastructures, there is a well-developed state-of-the-art for protection of Personally Identifiable Information (PII), incl. technologies, regulations, commercial software and services, the respective state-of-the-art for Open Infrastructures like the Internet and Web 2.0, i.e. online privacy, is rather immature. This is the result of basically three intertwined developments:

a) Regulations for online privacy are fragmented across more than 200 national legal systems and vary widely in their approaches and paradigms.
b) Personal data are monetized widely to finance a large industry for providing a rich spectrum of attractive and useful "free" services in Web 2.0. So there exists a fundamental dilemma, when user are interested in privacy <u>and</u> free services.
c) Behavioral profiling by data aggregators happens "behind" the ASPs visited by the user – typically invisible for the user and often without user consent

Recently, several papers were analyzing the flow of PII in the Internet/Web 2.0, resulting in the following key results:

- Current Online Social Networks are enabling the collection of PII (see http://www2.research.att.com/~bala/papers/wosn09.pdf)
- Browsers are storing more & more information incl. PII (see e.g. https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf)

Thus, the current level of PII leakages in Web 2.0 through browsers and other components is substantially limiting the enforcement of informational self-determination.

The challenge is how to control in Web 2.0 the flow of PII bypassing today's IDM and how to effectively enforce in Open Infrastructures the user's privacy rights and preferences.

So far, we have just identified this challenge and have no solution yet. E.g. for browsers there exist a number of approaches for tackling this problem, but most of these approaches have either a limited effectiveness, lack scalability, collide with principles of regulation (e.g. net neutrality), or are currently just infeasible:

Technological approaches for protecting the privacy of browser data include e.g.:

- Use (Firefox) Add-On's, see e.g. https://addons.mozilla.org/de/firefox/search?q=&cat=1%2C12
- Use (personal) proxy technology between browser & Internet
- Reduce storage of PII within the browser
- Certify privacy properties of JavaScript code used for Web 2.0
- Develop a browser with integrated enforcement of individual privacy policies for all personal data stored in the browser

There is some competing work: e.g. Mozilla Labs: Online Identity Concept Series
https://mozillalabs.com/blog/2010/03/online-identity-concept-series/
https://mozillalabs.com/conceptseries/identity/

The most **recent version of our slides is available online**:
http://www.dagstuhl.de/Materials/index.en.phtml?10141

→ **Please** send an email in case you are aware of any related work.

Further Reading

Cleaning Up After Cookies
Version 1.0
Katherine McKinley — kate[at]isecpartners[dot]com
https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf

Several Papers on PII Diffusion in the Internet & Web 2.0
by Balachander Krishnamurthy and co-authors
http://www2.research.att.com/~bala/papers/

PRIVACY ISSUES OF THE W3C GEOLOCATION API
Nick Doty, Deirdre K. Mulligan and Eric Wilde. (2010)
http://www.ischool.berkeley.edu/research/publications/2010/mulligan/privacy

Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naïve-Bayes Classifier
Herrmann, Dominik und Wendolsky, Rolf und Federrath, Hannes (2009)
http://epub.uni-regensburg.de/11919/

DESPERATELY SEEKING SOLUTIONS: USING
IMPLEMENTATION-BASED SOLUTIONS FOR THE
TROUBLES OF INFORMATION PRIVACY IN THE AGE
OF DATA MINING AND THE INTERNET SOCIETY
Tal Z. Zarsky
http://law.haifa.ac.il/techlaw/papers/Zarsky-Maine.pdf

CORPORATE PRIVACY TREND: THE “VALUE” OF PERSONALLY
IDENTIFIABLE INFORMATION (“PII”) EQUALS THE “VALUE”
OF FINANCIAL ASSETS
By: John T. Soma, J. Zachary Courson, and John Cadkin
http://jolt.richmond.edu/v15i4/Article11.pdf

Just Click Submit: The Collection, Dissemination and Tagging of Personally Identifying Information
Corey A. Ciocchetti, *University of Denver*
http://works.bepress.com/corey_ciocchetti/3/

It's Personal but Is It Mine? Toward Property Rights in Personal Information
Vera Bergelson, *Rutgers School of Law*
http://works.bepress.com/vera_bergelson/2/

On the future of (Online) Privacy Regulations
Address by Jennifer Stoddart
Privacy Commissioner of Canada
http://www.priv.gc.ca/speech/2010/sp-d_20100210_e.cfm