Controlling the Flow of PII to Web 2.0 beyond current Identity Services

Michael Marhöfer
Nokia Siemens Networks

Gökhan Bal
Goethe Universität Frankfurt

Disclaimer: This are the authors' personal views.

PrimeLife/IFIP Summer School 2010, Aug 2 - 6

Nokia Siemens Networks

Outline: More questions than answers

1. Introduction
2. Motivating **Online Privacy**
3. Definition of Online Privacy
4. Review of **Web Browser's** Privacy Mechanisms
5. Envisioning Online Privacy Services based on the User's Individual Privacy Preferences
6. **Key Challenges** towards Online Privacy
7. Outlook

Introduction

- Protection of PII **well developed** for closed Infrastructures.
- But **rather weak** in global, open Infrastructures like Web 2.0 due to
  - **Lack of globally accepted privacy regulations** for Web 2.0, …
  - **Browsers have to balance many interests, not just privacy**
  - **Personal data monetized** to finance a huge set of attractive and useful "**free" services** in Web 2.0 for billions of users
  - **Data aggregation and web analytics technologies quite mature**, often proprietary and not widely published
  - **Behavioral profiling & data collection** happens also behind the ASPs visited by a user, **mostly invisible** and without user consent
  - **Many users are not so aware of their online privacy**, are rather concerned with the services / their tangible benefits*

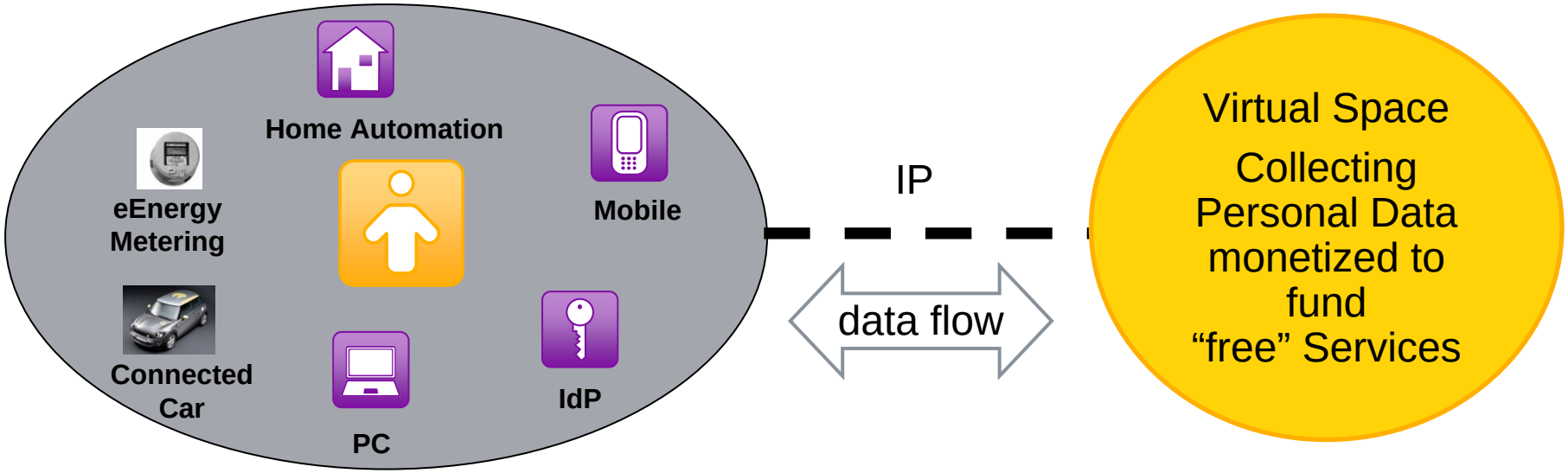
* See e.g. Alessandro Acquisti's research http://www.heinz.cmu.edu/~acquisti/research.htm

Motivating an Individual User's Online Privacy I

Motivation: Two aspects of a User's Online Privacy

A) Informational Self-Determination
User is **controlling the transfer of his personal data to parties in the virtual space**.

B) The right "to be left alone", according to the U.S. privacy law tradition:
User is **controlling the inflow of content, services, and advertisements** from the virtual space into the user's local environment



Motivating an Individual User's Online Privacy II: Examples of Typical Risks

- **Users** are transferring their own PII to ASPs and Service Providers, incl. (mobile) Online Social Networks
- **Identity Services** are transferring PII on behalf of users
- **For Web 2.0, also SPs, Data aggregators, and Web Analytics** are collecting & mining large amounts of (personal) data

See e.g.

- For a broad overview: **Helen Nissenbaum's** recent book "Privacy in context – Technology, Policy, and the integrity of Social Life", Part I on technology (pp. 21 – 66) http://www.sup.org/book.cgi?id=8862
- For several papers by **B. Krishnamurthy** on data collection & PII leakage: http://www2.research.att.com/~bala/papers/

Definition of an Individual User's Online Privacy

Part I (Outbound): Informational Self-Determination

For the outbound information flow, the user is exercising his right to informational self-determination, i.e. the **user is controlling the outflow of his information** (PII would be too narrow),
according to

- the locally applicable regulatory framework and
- his individual privacy preferences.

Part II (Inbound): The right to be left alone

For the inbound information flow, the user is exercising his right to be left alone, i.e. the **user is controlling the inflow of information** provided by parties in the virtual space,
according to

- the locally applicable regulatory framework and
- his individual privacy preferences.

Review of Web Browser's Privacy Mechanisms

- Browsers still the main interface between most user & Web, having a strong influence on the user's privacy
- Today's browsers offer quite some privacy mechanisms
  - Out-of-the-box features
  - Add-On's
- Special situation for mobile browsers (personal, location,…) not yet covered
- **Are such features helpful to ensure online privacy in an acceptable, convenient way?**
- **Caveat:**
  - Privacy features **often not configured / activated / installed** due to the user's lack of awareness / expertise of risks & technology,
  - or due to the user's preference for convenience & benefits

Out-of-the-box Privacy Mechanisms of Browsers

- (Privacy Mode: not leaving data trails on the device used) n/a
- Cookie Control — not effective
- Browser History Management — (+)
- Anti-Tracking (IE's "InPrivate Filtering") — cumbersome
- Manage Flash Shared Objects — no Web 2.0
- Blocking Script Execution — no Web 2.0
- Geolocation Control — +, if visible
- …

Add-On Privacy Mechanisms of Browsers

- Script Blockers like NoScript — effective, cumbersome
- Ad Blockers — + for inbound privacy
- Anonymization tools — - due to app. Layer
- Anti-Tracking Tools like Gostery — - inconvenient
- *What about trusting the sources of these tools?*

Summary:

- **Often not activated / configured / installed**
- **Most privacy machanisms ineffective or inconvenient**

Who is interested and able to improve browser privacy?

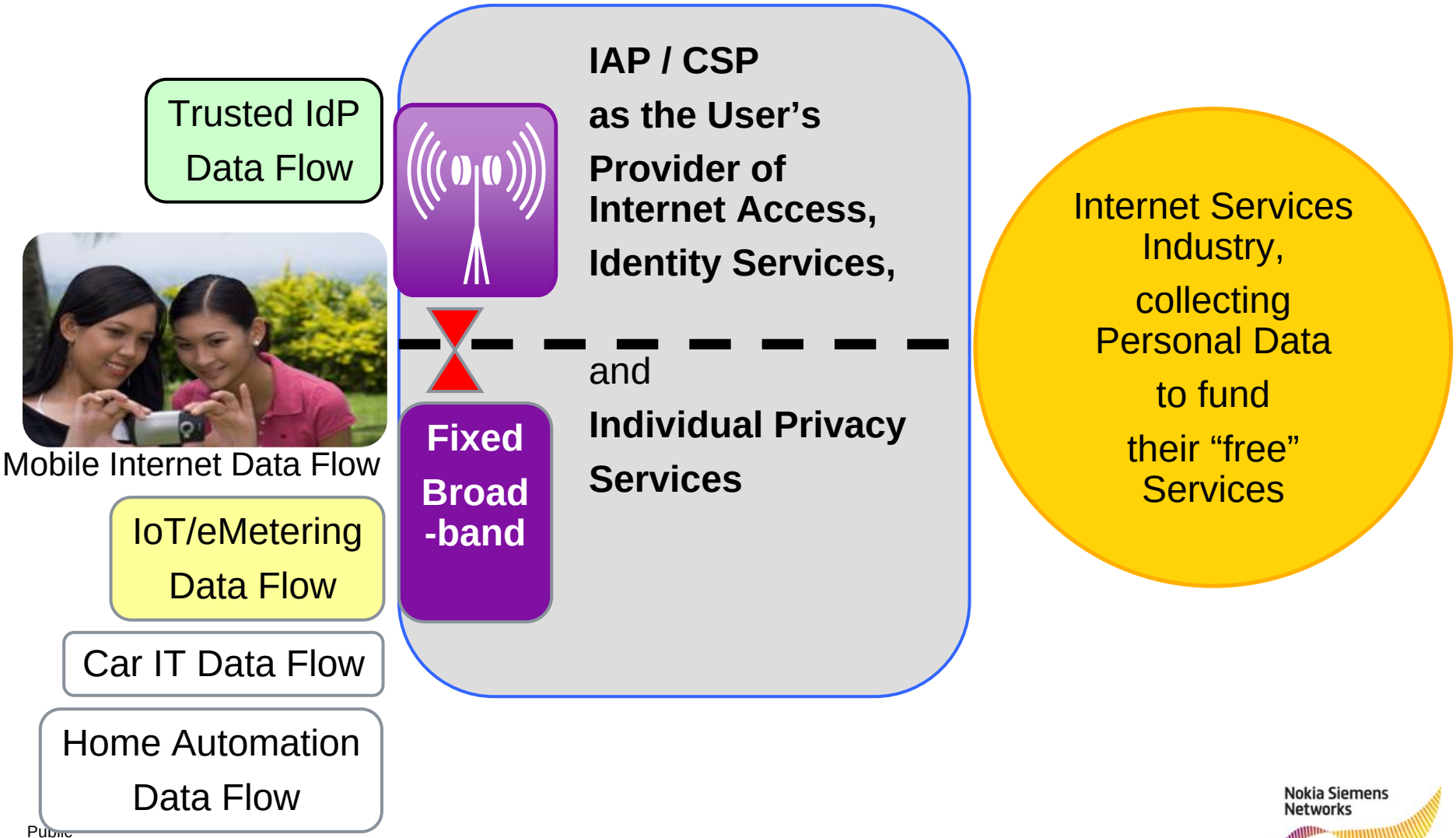
Users? Law? SPs? Browser manufacturers? IAP/CSP industry?

© Nokia Siemens Networks

Envisioning Online Privacy Services based on the User's Individual Privacy Preferences

- Enable the user to express in a convenient way his/her **individual online privacy preferences**
- Providers of Internet Access and Identity Services well-positioned to provide **privacy services controlling the user's data flow to the virtual space**
  - Registration and administration of user's online privacy preferences
  - Generation and enforcement of individual policies for
    - Identity Provisioning
    - **Data flows from/to the user's local environment to Web 2.0 etc. across various user devices**
- Also the user's **networked devices have to be adapted** accordingly (PEPs & interfaces to be added, …).

Envisioning Online Privacy Services based on the User's Individual Privacy Preferences



Outlining a Framework for Controlling the Flow of Information between the User and Web 2.0

- **Easy-to-use HCI/GUI** to express **individual privacy preferences** (a key technology)
- **User-centric identity management**, enabling provisioning of **individual** privacy services for IdP & other data flows
- Administration of the user's personal data and individual privacy preferences in a **Personal Data Portal** of the Internet Access Provider / CSPs
- **Automatic Transformation** of privacy preferences in executable policies
- **Customized Policy Decision Points** and **Policy Enforcement Points** for the **Identity Services** and the user's networked **devices and software** components

Can we today control the Outflow of the User's Personal Data in the Browser?

- **Aim**: **Let the user control the access** by remote parties in the virtual space **to PII in the user's local environment**
- **Scenario:**
  - User is trusting e.g. an **Internet Access Provider (IAP)**
  - IAP is also operating a **User-centric Identity Service**
  - IAP is also operating a **Personal Data Portal (PDP)** storing/referencing the user's data & privacy policies
  - User's **browser has been modified for interaction with the PDP** through a **customized PEP**
  - Let's assume: Each remote access through the browser to the user's data can be controlled by this PEP

Can we today control the Outflow of the User's Personal Data in the Browser?

How it should work:

Control of access by a remote party through the browser to user data according to an individual privacy policy

1. Remote party trying to access user data through the browser, e.g. user name, cookie, geo-location
2. Access request will be granted by the PEP according to the user's individual privacy policy administered by the Personal Data Portal.
3. Requested data is e.g. filtered or abstracted by the PEP according to the user's individual privacy policy.

Just one reason, why this does <u>not really</u> work today:

- Browser security features are an imperfect defense against active (JavaScript) components of Web 2.0 pages executed within the browser
- As complex software architectures with numerous plug-ins etc. can be exploited by these active elements to access data beyond the sand-box or the browser.

Key Challenges towards Online Privacy

Progress towards effective, convenient online privacy is **requires practical solutions of several challenges**:

1. **Create awareness** in industry and research for the dire state of online privacy
2. **Understand the technology** and **value network** for data collection, profiling and Web analytics in Web 2.0
3. **Influence regulatory frameworks to** also cover the privacy issues of browsers, data aggregation, behavioral profiling, Web analytics
4. **Develop HCI** for convenient expression of individual privacy policies
5. **Develop customized PEPs** for the enforcement of individual policies to control the remote access to a user's personal data
6. **Develop Personal Data Portals** for Internet Access Providers
7. **Evolve the browser's architecture and security features** to enable enforcement of individual privacy policies, e.g. by secure storage of personal user data in networked devices (first step: feasibility demo)

Outlook: Establishing Individual Privacy Services by Internet Access Providers

- Establishing online privacy services by IAPs/CSPs has the potential to modify the well-established value network around Web 2.0's "free" services.
- Only a co-ordinated set of activities has the chance to overcome inertia towards establishing privacy services by IAPs/CSPs for the Internet and Web 2.0 :
  1. Substantial progress in technology for implementing online privacy
  2. Corresponding regulatory changes
  3. Subsequent standardization of affected interfaces
  4. Coordinated action by the IAP/CSP industry

Who of you is able to contribute hints / references / …?

Contact:

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

Gökhan Bal goekhan.bal@m-chair.net
Goethe Universitaet Frankfurt
Grüneburgplatz 1, 60323 Frankfurt

Introducing a few Acronyms

- **PII**: Personally Identifiable Information
- **IAP: Internet Access Provider**
- **CSP: Communication Service Provider**: provider of communication services, e.g. mobile operator, fixed-line operator
- **Identity (ID)**: a set of Personally Identifiable Information
- **User-centric Identity Management** (**UCIDM**):
  User-controlled Management of Identity information for the user's online interaction with all kinds of Service Providers
- **IdP**: Provider of Identity Services

Today's NSN's Identity Management Solution

Identity Management Features

- Simplified Experience
- 1 User multi-identities
- Protected & managemented User Privacy
- Personalized ads-services

- Web single sign-on, incl. zero-single sign-on
- Federation, persistent, temporary, anonymous
- Authentication, network based, 2-factor-authn
- End-User Profile Access for federated services
- Authorization, policies per user & partner, PDP

- Business Transformation & 2 sided business models
- Faster time to service revenue
- Lower cost infrastructure for Identity Management
- Anonymous brokering to 3rd parties, i.e. legal age
- Personalized ads-services
- Customer Privacy enablement
- New Use Case enablement
- Increased Loyalty

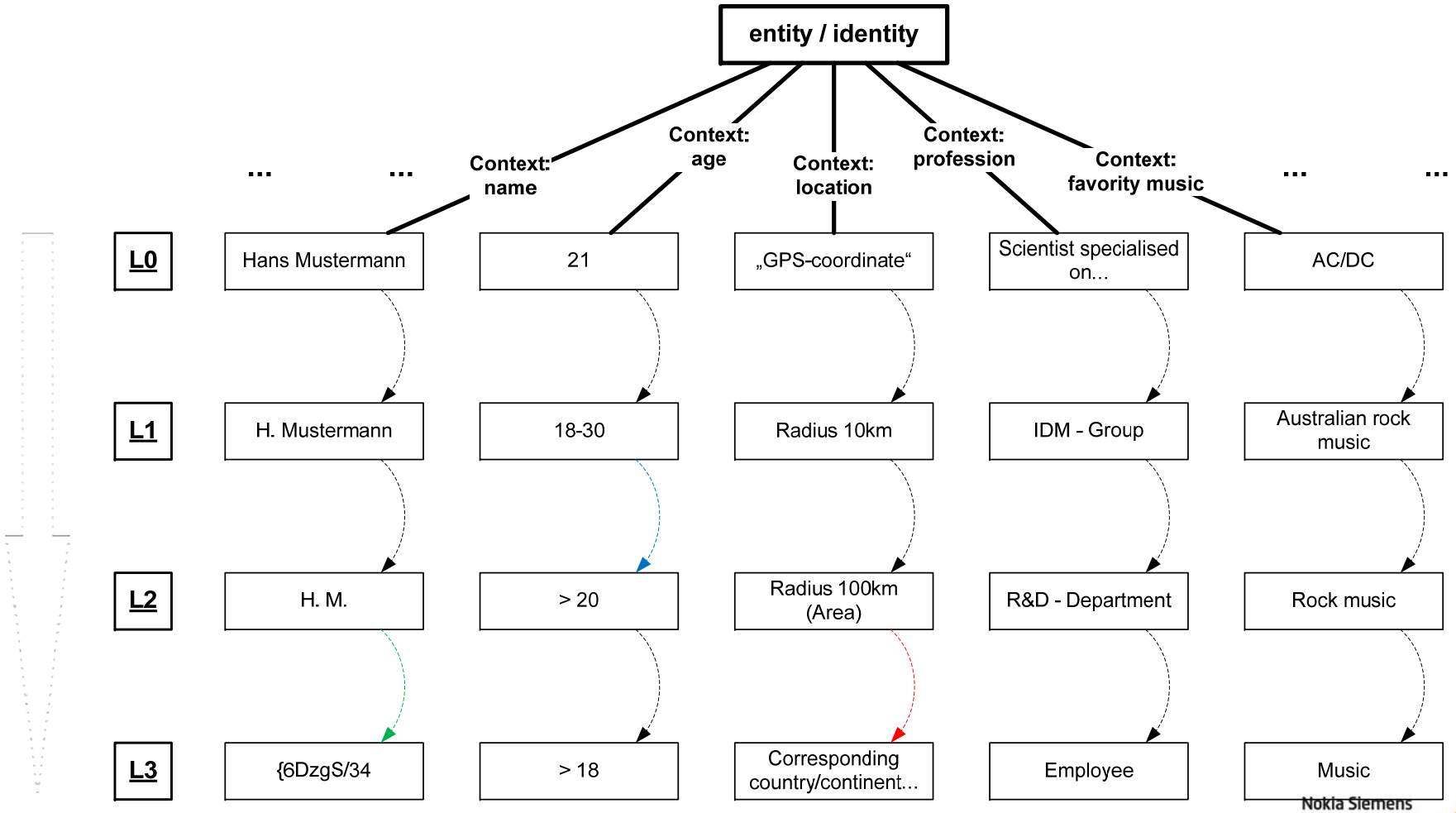
- Personalized relevant service delivery
- Enhanced mobility-device support
- Target Advertising
- Payment transaction assurance

© Nokia Siemens Networks

Levels of Privacy (LoP) for Identity Attributes

Source: Presentation by Michael Marhöfer
http://www.dagstuhl.de/Materials/index.en.phtml?10141

From concrete, personal attributes to attributes of a growing group



© Nokia Siemens Networks

Some More References

On Data Storage in Browsers:

https://www.isecpartners.com/files/iSEC_Cleaning_Up_After_Cookies.pdf

On PII Diffusion in the Internet & Web 2.0:

http://www2.research.att.com/~bala/papers/

On Diffusion of Geolocation Data:

http://www.ischool.berkeley.edu/research/publications/2010/mulligan/privacy

On the Ineffectiveness of some PETs in the Internet:

http://epub.uni-regensburg.de/11919/

Privacy papers in Law Journals (long, but quite informative):

http://law.haifa.ac.il/techlaw/papers/Zarsky-Maine.pdf

http://jolt.richmond.edu/v15i4/Article11.pdf

http://works.bepress.com/corey_ciocchetti/3/

http://works.bepress.com/vera_bergelson/2/

On the future of (Online) Privacy Regulations:

http://www.priv.gc.ca/speech/2010/sp-d_20100210_e.cfm

Nokia Siemens Networks