Privacy and Identity Management for Life
Michele Bezzi, Penny Duquenoy, Simone Fischer-Hübner, Marit Hansen

To cite this version:

HAL Id: hal-01556293
https://inria.hal.science/hal-01556293
Submitted on 4 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
Editor-in-Chief

A. Joe Turner, Seneca, SC, USA

Editorial Board

Foundations of Computer Science
Mike Hinchey, Lero, Limerick, Ireland

Software: Theory and Practice
Bertrand Meyer, ETH Zurich, Switzerland

Education
Bernard Cornu, CNED-EIFAD, Poitiers, France

Information Technology Applications
Ronald Waxman, EDA Standards Consulting, Beachwood, OH, USA

Communication Systems
Guy Leduc, Université de Liège, Belgium

System Modeling and Optimization
Jacques Henry, Université de Bordeaux, France

Information Systems
Barbara Pernici, Politecnico di Milano, Italy

Relationship between Computers and Society
Chrisanthi Avgerou, London School of Economics, UK

Computer Systems Technology
Paolo Prinetto, Politecnico di Torino, Italy

Security and Privacy Protection in Information Processing Systems
Kai Rannenberg, Goethe University Frankfurt, Germany

Artificial Intelligence
Max A. Bramer, University of Portsmouth, UK

Human-Computer Interaction
Annelise Mark Pejtersen, Center of Cognitive Systems Engineering, Denmark

Entertainment Computing
Ryohei Nakatsu, National University of Singapore
IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP’s aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

*IFIP’s mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.
New Internet developments pose greater and greater privacy dilemmas. In the Information Society, the need for individuals to protect their autonomy and retain control over their personal information is becoming more and more important. Today, information and communication technologies—and the people responsible for making decisions about them, designing, and implementing them—scarcely consider those requirements, thereby potentially putting individuals’ privacy at risk. The increasingly collaborative character of the Internet enables anyone to compose services and contribute and distribute information. It may become hard for individuals to manage and control information that concerns them and particularly how to eliminate outdated or unwanted personal information, thus leaving personal histories exposed permanently. These activities raise substantial new challenges for personal privacy at the technical, social, ethical, regulatory, and legal levels: How can privacy in emerging Internet applications such as collaborative scenarios and virtual communities be protected? What frameworks and technical tools could be utilized to maintain life-long privacy?

During September 3–10, 2009, IFIP (International Federation for Information Processing) working groups 9.2 (Social Accountability), 9.6/11.7 (IT Misuse and the Law), 11.4 (Network Security) and 11.6 (Identity Management) held their 5th International Summer School in cooperation with the EU FP7 integrated project PrimeLife in Sophia Antipolis and Nice, France. The focus of the event was on privacy and identity management for emerging Internet applications throughout a person’s lifetime.

The aim of the IFIP Summer Schools has been to encourage young academic and industry entrants to share their own ideas about privacy and identity management and to build up collegial relationships with others. As such, the Summer Schools have been introducing participants to the social implications of information technology through the process of informed discussion.

Following the holistic approach advocated by the involved IFIP working groups and by the PrimeLife project, a diverse group of participants ranging from young doctoral students to leading researchers in the field engaged in discussions, dialogues and debates in an informal and supportive setting. The interdisciplinary, and international, emphasis of the Summer School allowed for a broader understanding of the issues in the technical and social spheres.

All topical sessions started with introductory lectures by invited speakers in the mornings, followed by parallel workshops and seminars in the afternoons. The workshops consisted of short presentations based on the contributions submitted by participating PhD students, followed by active discussions.

Contributions combining technical, social, ethical or legal perspectives were solicited. Keynote speeches provided the focus for the theme of the Summer School—Lifelong Privacy, Privacy Aspects of Social Networks, Privacy of Data,
Transparency and Data subject Access, Privacy Principles for Identity Management, Economic Privacy Aspects, Identity and Legal, Technical and Economic Aspects of a new regulatory Framework—and the contributions from participants enhanced the ideas generated by the keynote speeches. The Summer School was a very successful event. More than 50 delegates from more than 15 countries actively participated. We succeeded in initiating intensive discussions between PhD students and established researchers from different disciplines.

These proceedings include both keynote papers and submitted papers accepted by the Program Committee, which were presented at the Summer School. The review process consisted of two steps. In the first step, contributions for presentation at the Summer School were selected based on reviews of submitted short papers by the Summer School Program Committee. The second step took place after the Summer School, when the authors had an opportunity to submit their final full papers addressing discussions at the Summer School. The submissions were again reviewed, by three reviewers each, and those included in these proceedings were carefully selected by the International Summer School Program Committee and by additional reviewers according to common quality criteria.

It is our pleasure to thank the members of the Program Committee, the additional reviewers, the members of the Organizing Committee as well as all the speakers. Without their work and dedication, this Summer School would not have been possible. Last but not least, we owe special thanks to the PrimeLife project, SAP, Microsoft Research, Eurecom, HumanIT at Karlstad University as well as IFIP for their support.

March 2010

Michele Bezzi
Penny Duquenoy
Simone Fischer-Hübner
Marit Hansen
The PrimeLife/IFIP Summer School 2009 was organized by the EU FP7 Project PrimeLife and the IFIP Working Groups 9.2, 9.6/11.7, 11.4 and 11.6.

General Chair

Michele Bezzi  
SAP Research, France

Program Committee Co-chairs

Penny Duquenoy  
Middlesex University, UK, IFIP WG 9.2 Chair
Simone Fischer-Hübner  
Karlstad University, Sweden, IFIP WG11.6  
Vice Chair
Marit Hansen  
Independent Centre for Privacy Protection  
Schleswig-Holstein, Kiel, Germany

Organizing Committee Chair

Jean-Christophe Pazzaglia  
SAP Research, France

Program Committee

Jan Camenisch  
IBM Research, Switzerland, IFIP WP 11.4 Chair
Mark Gasson  
University of Reading, UK
Hans Hedbom  
Karlstad University, Sweden
Tom Keenan  
University of Calgary, Canada
Dogan Kesdogan  
Siegen University, Germany
Kai Kimppa  
University of Turku, Finland
Eleni Kosta  
KU Leuven, Belgium
Ronald Leenes  
Tilburg University, The Netherlands
Elisabeth de Leeuw  
Ordina, The Netherlands, IFIP WG 11.6 Chair
Marc van Lieshout  
Joint Research Centre, Spain
Javier Lopez  
University of Malaga, Spain
Vaclav Matyas  
Masaryk University, Brno, Czech Republic
Martin Meints  
Independent Centre for Privacy Protection  
Schleswig-Holstein, Kiel, Germany
Jean-Christophe Pazzaglia  
SAP Research, France
Uli Pinsdorf  
Europäisches Microsoft Innovations Center GmbH/EMIC, Germany
Andreas Pfitzmann  
TU Dresden, Germany
VIII Organization

Charles Raab University of Edinburgh, UK
Kai Rannenberg Goethe University Frankfurt, Germany, IFIP TC11 Chair
Dieter Sommer IBM Research, Switzerland
Sandra Steinbrecher TU Dresden, Germany
Morton Swimmer John Jay College of Criminal Justice, CUNY, USA
Jozef Vyskoc VaF, Slovakia
Rigo Wenning W3C, France
Diane Whitehouse The Castlegate Consultancy, UK
Pierangela Samarati Milan University, Italy
Gregory Neven IBM Research Zurich, Switzerland

Additional Reviewers

Sebastian Clauß TU Dresden, Germany
Benjamin Kellermann TU Dresden, Germany
Katrin Borcea-Pfitzmann TU Dresden, Germany
# Table of Contents

## Lifelong Privacy

Lifelong Privacy: Privacy and Identity Management for Life  
(Keynote Paper) ............................................................... 1  
_Andreas Pfitzmann and Katrin Borcea-Pfitzmann_

Delegation for Privacy Management from Womb to Tomb – A European  
Perspective ................................................................. 18  
_Marit Hansen, Maren Raguse, Katalin Storf, and Harald Zwingelberg_

Saving On-Line Privacy (Keynote Paper) ......................... 34  
_Jan Camenisch and Gregory Neven_

## Privacy for Social Network Sites and Collaborative Systems

Context Is Everything: Sociality and Privacy in Online Social Network  
Sites (Keynote Paper) ..................................................... 48  
_Ronald Leenes_

The Freddi Staurs of Social Networking – A Legal Approach  
(Keynote Paper) ............................................................ 66  
_Eleni Kosta_

Facebook and Its EU Users – Applicability of the EU Data Protection  
Law to US Based SNS ......................................................... 75  
_Aleksandra Kuczerawy_

On the Security and Feasibility of Safebook: A Distributed  
Privacy-Preserving Online Social Network (Keynote Paper) .... 86  
_Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe_

Privacy-Respecting Access Control in Collaborative Workspaces . 102  
_Stefanie Pötzsch and Katrin Borcea-Pfitzmann_

## Privacy for eGovernment Applications

A Three-Dimensional Framework to Analyse the Governance of  
Population Registers .......................................................... 112  
_José Formaz and Olivier Glassey_

Use of ePassport for Identity Management in Network-Based  
Citizen-Life Processes ....................................................... 122  
_Pravir Chawdhry and Ioannis Vakalis_
The Use of Privacy Enhancing Technologies for Biometric Systems
Analysed from a Legal Perspective ........................................ 134

Els J. Kindt

Privacy and Identity Management for eHealth and
Ambient Assisted Living Applications
Assuring Privacy of Medical Records in an Open Collaborative
Environment - A Case Study of Walloon Region’s eHealth Platform .... 146
Syed Naqvi, Gautier Dallons, Arnaud Michot, and
Christophe Ponsard

Goal-Oriented Access Control Model for Ambient Assisted Living ...... 160
Fabio Massacci and Viet Hung Nguyen

Anonymisation and Privacy-Enhancing Technologies
Privacy of Outsourced Data (Keynote Paper) .......................... 174
Sabrina De Capitani di Vimercati and Sara Foresti

Sharing Data for Public Security ............................................. 188
Michele Bezzi, Gilles Montagnon, Vincent Salzgeber, and
Slim Trabelsi

An Analysis for Anonymity and Unlinkability for a VoIP
Conversation ............................................................................ 198
Ge Zhang

PRIvacy LEakage Methodology (PRILE) for IDS Rules ............... 213
Nils Ulltveit-Moe and Vladimir Oleshchuk

Identity Management and Multilateral Security
Digital Personae and Profiles as Representations of Individuals ....... 226
Arnold Roosendaal

Anonymous Credentials in Web Applications: A Child’s Play with the
PRIME Core ............................................................................. 237
Benjamin Kellermann and Immanuel Scholz

Reaching for Informed Revocation: Shutting Off the Tap on Personal
Data .......................................................................................... 246
Ioannis Agrafiotis, Sadie Creese, Michael Goldsmith, and
Nick Papanikolaou

Multilateral Privacy in Clouds: Requirements for Use in Industry ...... 259
Ina Schiering and Markus Hansen
Usability, Awareness and Transparency Tools

PET-USES: Privacy-Enhancing Technology – Users’ Self-Estimation
Scale ............................................................... 266
   Erik Wästlund, Peter Wolkerstorfer, and Christina Köffel

Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services ................. 275
   André Deuker

Secure Logging of Retained Data for an Anonymity Service ............... 284
   Stefan Köpsell and Petr Švenda

Adding Secure Transparency Logging to the PRIME Core .................. 299
   Hans Hedbom, Tobias Pulls, Peter Hjärtquist, and Andreas Lavén

Author Index .................................................. 315