

Editor-in-Chief

*A. Joe Turner, Seneca, SC, USA*

Editorial Board

Foundations of Computer Science

*Mike Hinchey, Lero, Limerick, Ireland*

Software: Theory and Practice

*Michael Goedicke, University of Duisburg-Essen, Germany*

Education

*Arthur Tatnall, Victoria University, Melbourne, Australia*

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

*Jan Pries-Heje, Roskilde University, Denmark*

ICT and Society

*Jackie Phahlamohlaka, CSIR, Pretoria, South Africa*

Computer Systems Technology

*Paolo Prinetto, Politecnico di Torino, Italy*

Security and Privacy Protection in Information Processing Systems

*Kai Rannenber, Goethe University Frankfurt, Germany*

Artificial Intelligence

*Tharam Dillon, Curtin University, Bentley, Australia*

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.

Jan Camenisch Bruno Crispo  
Simone Fischer-Hübner Ronald Leenes  
Giovanni Russello (Eds.)

# Privacy and Identity Management for Life

7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife  
International Summer School  
Trento, Italy, September 5-9, 2011  
Revised Selected Papers

## Volume Editors

Jan Camenisch  
IBM Zurich Research Laboratory  
 Säumerstr. 4, 8803 Rüschlikon, Switzerland  
E-mail: jca@zurich.ibm.com

Bruno Crispo  
University of Trento  
Department of Information Engineering and Computer Science  
Via Sommarive, 14, 38123 Povo (TN), Italy  
E-mail: crispo@disi.unitn.it

Simone Fischer-Hübner  
Karlstad University, Department of Computer Science  
Universitetsgatan 1, 65188 Karlstad, Sweden  
E-mail: simone.fischer-huebner@kau.se

Ronald Leenes  
Tilburg University  
Tilburg Institute for Law, Technology, and Society (TILT)  
PO Box 90153, 5000 LE Tilburg, The Netherlands  
E-mail: r.e.leenes@uvt.nl

Giovanni Russello  
The University of Auckland, Computer Science Department  
Private Bag 92019, Auckland 1142, New Zealand  
E-mail: g.russello@auckland.ac.nz

ISSN 1868-4238 e-ISSN 1868-422X  
ISBN 978-3-642-31667-8 e-ISBN 978-3-642-31668-5  
DOI 10.1007/978-3-642-31668-5  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012941094

CR Subject Classification (1998): C.2, K.6.5, D.4.6, E.3, H.4, J.1

© IFIP International Federation for Information Processing 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Preface

Internet applications, such as Web 2.0 applications and cloud computing, increasingly pose privacy dilemmas. When they communicate over the Internet, individuals leave trails of personal data which may be stored for many years to come. These developments raise substantial new challenges for personal privacy at the technical, social, ethical, regulatory, and legal levels: How can privacy be protected in emerging Internet applications such as collaborative scenarios and virtual communities? What frameworks and tools could be used to gain, regain, and maintain informational self-determination and lifelong privacy?

Such questions were addressed by the 7th IFIP Summer School on Privacy and Identity Management for Emerging Internet Applications throughout a person's lifetime. This multidisciplinary summer school was held September 5–9, 2011, in Trento by the IFIP (International Federation for Information Processing) working groups 9.2, 9.6/11.7, 11.4, and 11.6 in cooperation with the PrimeLife project consortium and the projects ABC4Trust, e-Me, Endorse, NES-SOS, TAS3, PETweb II, and U-PrIm (in cooperation with HumanIT).

The aim of the IFIP Summer School is traditionally manifold: to increase the research community in privacy and identity management, to further research, and to enable the update of privacy-enhancing technology. The summer school takes a holistic approach to technology and supports interdisciplinary exchange. In particular, participants' contributions that combine technical, legal, regulatory, socio-economic, ethical, philosophical, or psychological perspectives are sought. To this end, the summer school encourages young researchers to share their own ideas about privacy and identity management, to meet and liaise with colleagues, and to present and discuss their research results with senior researchers. The summer school also brings together senior researchers from all disciplines of privacy and identity management and stimulates a holistic discussion and exchanges of ideas. In support of this, the summer school features a number of inspirational keynotes leading to discussion.

This year, we had the pleasure of keynotes by Alessandro Armando, David Chadwick, Andrea Di Nicola, Peter Gullberg, Marit Hansen, Riitta Hellman, Thomas Patrick Keenan, Eleni Kosta, Gregory Neven, Charles Raab, and Sarah Spiekerman. Thanks to all of them for their excellent presentations and for contribution to the atmosphere and success of the summer school!

Complementing the keynotes, the summer school featured 18 parallel workshops, which were dedicated to the presentation and discussion of the papers selected from the submission with five exceptions: One workshop was held as a rump session, one workshop was a tutorial on *Cryptography for Privacy* by Jan Camenisch and Gregory Neven and two workshops were open exploration and discussion of a dedicated topic: one on *Contextual Integrity: A Means to Manage Privacy* led by Katrin Borcea-Pfitzmann and Marit Hansen and one on *Addressing Ethical Issues*

*Using Scenarios in European Technology Development Projects* led by Aygen Kurt and Penny Duquenoy. Furthermore, onw workshop organized by Riitta Hellman discussed ICT for persons with dementia and related privacy issues.

This book contains the thoroughly refereed post-conference proceedings of the summer school. In particular, it contains revised papers selected from numerous submissions. In the first round, submitted papers were reviewed and selected for presentation at the summer school. Most of these papers were revised based on the comments and discussion at the summer school and underwent a second round of review, selection, and revision to be included in the present proceedings. In addition to these papers, the proceedings contain two keynote papers: *Top 10 Mistakes in System Design from a Privacy Perspective* by Marit Hansen and *Are They Making Our Privates Public? - Emerging Risks of Governmental Open Data Initiatives* by Tom Keenan. Finally, the Program Committee Chairs selected the paper entitled *Data Protection Authorities in a Comparative Perspective* by Philip Schütz for the Best Student Paper Award. Congratulations Philip!

We express our gratitude to the numerous people who made the summer school such a success: all the authors who submitted papers, the keynote speakers and the participants, and the Organizing Committee members. Thank you!

March 2012

Jan Camenisch  
Bruno Crispo  
Simone Fischer-Hübner  
Ronald Leenes  
Giovanni Russello

# Organization

The IFIP Summer School 2011 was organized by the IFIP (International Federation for Information Processing) working groups 9.2, 9.6/11.7, 11.4, and 11.6 in cooperation with the PrimeLife project consortium and the European research projects ABC4Trust, e-Me, Endorse, NESSOS, TAS3, as well as the Norwegian PETweb II project and the Swedish U-PrIM project (in cooperation with HumanIT).

## Program Co-chairs

Jan Camenisch	IBM Research – Zurich, Switzerland
Simone Fischer-Huebner	Karlstad University, Sweden
Ronald Leenes	Tilburg University, The Netherlands

## General Summer School Chair

Bruno Crispo	University of Trento, Italy
Marc van Lieshout	TNO, The Netherlands

## Organizing Committee Chair

Giovanni Russello	Create-Net, Italy
-------------------	-------------------

## Program Committee

Bibi van der Berg	Tilburg University, The Netherlands
Michele Bezzi	SAP Research, France
Gabriela Bodea	TNO, The Netherlands
Katrin Borcea-Pfutzmann	TU Dresden, Germany
Pedro Bueso	University of Zaragoza, Spain
Changyu Dong	Strathclyde University, UK
Penny Duquenoy	Middlesex University, UK
Pierfranco Ferronato	Soluta.net, Italy
Lothar Fritsch	Norwegian Computer Center, Norway
Mark Gasson	University of Reading, UK
Marit Hansen	UDL, Germany
Hans Hedbom	Karlstad University, Sweden
Thomas Heistracher	SUAS, Austria
Jaap-Henk Hoepman	TNO, The Netherlands
Tom Keenan	University of Calgary, Canada
Dogan Kesdogan	Siegen University, Germany

Kai Kimppa	University of Turku, Finland
Linda Kool	TNO, The Netherlands
Eleni Kosta	KU Leuven, Belgium
Paul Malone	Waterford Institute of Technology, Ireland
Leonardo Martucci	CASED, Germany
Vaclav Matyas	Masaryk University, Brno, Czech Republic
Gregory Neven	IBM Research – Zurich, Switzerland
Stefano Paraboschi	University of Bergamo, Italy
Uli Pinsdorf	EMIC, Germany
Charles Raab	University of Edinburgh, UK
Kai Rannenber	Goethe University Frankfurt, Germany
Norberto Patrignani	Catholic University of Milan, Italy
Pierangela Samarati	Milan University, Italy
Einar Arthur Snekenes	Gjovik University College, Norway
Dieter Sommer	IBM Research – Zurich, Switzerland
Morton Swimmer	Trend Micro, USA
Jozef Vyskoc	VaF, Slovakia
Rigo Wenning	W3C, France
Diane Whitehouse	The Castlegate Consultancy, UK
Erik Wästlund	Karlstad University, Sweden

### **Additional Reviewers**

Jörg Daubert	CASED, Germany
Thomas Lampoltshammer	University of Salzburg, Austria

# List of Keynotes Given at the Summer School

*Lifelong Privacy: The Right to be Forgotten?*

Charles Raab (Edinburgh University)

*Inclusive Identity Management in new Social Media*

Riitta Hellman (Karde AS / Norwegian Computing Center)

*Sticky Policies*

David Chadwick (University of Kent)

*Privacy Impact Assessments and Privacy by Design - Ways to go forward*

Sarah Spiekermann (WU Vienna)

*Usable Privacy-enhanced mobile Identity Management*

Peter Gullberg (Gemalto)

*Privacy and Security for Mobile Phones*

Jean-Pierre Seifert (TU Berlin)

*Privacy Protection Goals and Top 10 Mistakes in System Design from a Privacy Perspective*

Marit Hansen (Vice Data Protection Commissioner/ULD)

*Are They Making Our Privates Public? - Emerging Risks of Governmental Open Data Initiatives*

Tom Keenan (University of Calgary)

*Tracking trends: Location Tracking and Do Not Track*

Eleni Kosta (KU Leuven)

*Identity Thefts and Identity Managment: Criminological and Legal Aspects*

Andrea De Nicola (University of Trento)

*Security and Privacy of Web-based Single Sign-On Protocols: Pitfalls and Solutions*

Allessandro Armando (FBK)

# Table of Contents

## Invited Talks

- Are They Making Our Privates Public? – Emerging Risks of  
Governmental Open Data Initiatives ..... 1  
*Thomas P. Keenan*
- Top 10 Mistakes in System Design from a Privacy Perspective and  
Privacy Protection Goals ..... 14  
*Marit Hansen*

## Privacy Metrics and Comparison

- Developing a Strategy for Automated Privacy Testing Suites ..... 32  
*Ioannis Agraftotis, Sadie Creese, and Michael Goldsmith*
- Assessing Formal Independence of Data Protection Authorities in a  
Comparative Perspective ..... 45  
*Philip Schütz*

## Policies

- Extracting Access Control and Conflict Resolution Policies from  
European Data Protection Law ..... 59  
*Kaniz Fatema, David W. Chadwick, and Brendan Van Alsenoy*
- Early Lessons Learned in the ENDORSE Project: Legal Challenges  
and Possibilities in Developing Data Protection Compliance Software ... 73  
*Sandra Orlislaegers*

## Privacy and Transparency in the Age of Cloud Computing

- The Infrastructure Level of Cloud Computing as a Basis for Privacy  
and Security of Software Services ..... 88  
*Ina Schiering and Jan Kretschmer*
- (More) Side Channels in Cloud Storage: Linking Data to Users ..... 102  
*Tobias Pulls*
- Who Got All of My Personal Data? Enabling Users to Monitor the  
Proliferation of Shared Personally Identifiable Information ..... 116  
*Sebastian Labitzke*

**Privacy for Mobile Applications**

Exploring Touch-Screen Biometrics for User Identification on Smart Phones ..... 130  
*Julio Angulo and Erik Wästlund*

Using a Smartphone to Access Personalized Web Services on a Workstation ..... 144  
*Faysal Boukayoua, Jan Vossaert, Bart De Decker, and Vincent Naessens*

Designing Privacy-Enhancing Mobile Applications ..... 157  
*Koen Decroix, Bart De Decker, and Vincent Naessens*

**Consumer Privacy**

Extending Comparison Shopping Sites by Privacy Information on Retailers ..... 171  
*Ulrich König and Marit Hansen*

Do-Not-Track Techniques for Browsers and Their Implications for Consumers ..... 187  
*Martin Beck and Michael Marhöfer*

**Privacy for Online Communities**

P2P Social Networks with Broadcast Encryption Protected Privacy .... 197  
*Oleksandr Bodriagov and Sonja Buchegger*

Privacy by Design: Does It Matter for Social Networks?..... 207  
*Mohammad Badiul Islam and Renato Iannella*

**Privacy for eHealth and eID Applications**

Privacy Preserving Mechanisms for a Pervasive eHealth System ..... 221  
*Milica Milutinovic, Koen Decroix, Vincent Naessens, and Bart De Decker*

Formalising Requirements for a Biobank Case Study Using a Logic for Consent and Revocation ..... 232  
*Ioannis Agraftotis, Sadie Creese, and Michael Goldsmith*

Privacy Protection Goals and Their Implications for eID Systems ..... 245  
*Harald Zwingelberg and Marit Hansen*

## Privacy Attacks and Problems

Avoiding Man-in-the-Middle Attacks When Verifying Public Terminals .....	261
<i>Gergely Alpár and Jaap-Henk Hoepman</i>	
Massive Data Collection by Mistake? .....	274
<i>Arnold Roosendaal</i>	

## Ethics

Addressing Governance and Ethics in European Technology Development Projects through Scenarios .....	283
<i>Aygen Kurt and Penny Duquenoy</i>	
<b>Author Index</b> .....	293