Annual Privacy Forum 2016

Final Report

OCTOBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For contacting the authors please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

We thank all participants and PC members that made APF 2016 a success.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

© European Union Agency for Network and Information Security (ENISA), 2016
Reproduction is authorised provided the source is acknowledged.

Table of Contents

1. Introduction

Nowadays electronic communication networks and digital services are an essential part of an increasing number of everyday commodities. In the era of automated profiling and electronic surveillance, citizens face a serious threat against their right to privacy and informational self-determination, especially when using the internet and mobile services. The lack of transparency regarding the functionality and interconnection of such services increases the risk of uncontrollable processing of personal data. In this regard, the upcoming Data Protection Regulation will be a useful instrument to protect the privacy of individuals. However, for its successful implementation, this new framework needs to be enforced by proper technologies and encompassed with sustainable business models along with mechanisms to promote privacy awareness and help users to understand the value of their data.

In light of the data protection regulation and the European digital agenda, DG CONNECT, EDPS, ENISA and, Goethe University Frankfurt organized APF 2016 (http://privacyforum.eu/). APF 2016 was held 7 & 8 September at Goethe University Frankfurt am Main, Germany. The event encouraged dialog with key note speakers, panel discussions, and provided room for exchange of ideas in between scientific sessions. The proceedings, LNCS 9857[1], are available online; a print version was distributed to relevant stakeholders (participants and management board).

There conference was attended by more than 100 registered participants.

[1] http://link.springer.com/book/10.1007%2F978-3-319-44760-5

2. Programme

2.1 Invited talks

Three speakers from industry were invited, namely Thomas Kremer, Deutsche Telekom AG, Mikko Hypponen, F-Secure, and Jacoba Sieders ABN AMRO Bank. Keynotes aimed to fuel the discussion from a practical perspective, while the closing note aimed to give home work to researchers and policy makers. The invited speakers are listed below.

Dr. Thomas Kremer has been the Board of Management member responsible for Data Privacy, Legal Affairs and Compliance at Deutsche Telekom AG since June 2012. He was the interim Chief Human Resources Officer from January 2014 to March 2015.

Previously, he worked for ThyssenKrupp AG where he became General Counsel of the holdings' legal department in 2003, and Chief Compliance Officer of the ThyssenKrupp Group in 2007. In 2009, Thomas Kremer assumed leadership of the newly formed Corporate Center Legal & Compliance. He was appointed Executive Vice President (Generalbevollmächtigter) in 2011.

In addition to his experience in industry, Thomas Kremer worked as a research assistant at the University of Bonn, where he gained a doctorate in law in 1994. Moreover, he is engaged in the governmental commission German Corporate Governance Codex (Deutscher Corporate Governance Kodex DCGK). Since November 2015 he is chairman of the network safety association "Deutschland sicher im Netz" (Making Germany safe on the Net

Mikko Hypponen is the Chief Research Officer of F-Secure. He's been with the company since 1991.

Mr. Hypponen has written on his research for the New York Times, Wired and Scientific America and he appears frequently on international TV. He has lectured at the universities of Stanford and Cambridge and he has delivered the most watched computer security talk on the internet.

Mr. Hypponen is a member of the board of the Nordic Business Forum and a member of the advisory board of T2.

Jacoba Sieders. As executive within the ABN AMRO Corporate Information Security Office, Jacoba has final accountability for digital identity and the online and mobile access control for customers, employees and partners for the bank’s data and infrastructure. Next to that she holds the research and innovation portfolio for the domain. Since seventeen years she has been running security and identity management in three major global banks, and she is experienced in designing data protection frameworks and governance from the security and identity perspective. Today’s main topics on her agenda are API banking, data centric security, identity management for block chain and hybrid clouds, inter-bank identity programs, the Payment Services Directive II requirements, and the new concepts for authentication which ABN AMRO is developing. Jacoba is a member of the advisory board of the independent European think-tank ID-Next and is regularly peaking on the topic.

2.2 Panels

The 3 panels aimed to promote ENISA's projects. With APF late in the year, they could be seen as a first peer review of the relevant projects. However, since we want to move APF to an earlier time of the year, in the future panel discussions will evolve more into kick-off or brain storming discussions nevertheless tightly coupled to ENISA WP activities. Moreover, they could be used to aim for a more multiannual strategy, evaluating past years projects and collecting ideas for how to continue a certain work stream.

2.2.1 Online privacy tools for the general public

It is widely recognised that one of the most serious concerns today is the preservation of privacy when using internet and mobile applications. This concern has given rise to an increasing appearance of online tools, often open-source and/or freeware, affirming that they can offer certain privacy-preventive functionality, such as for example secure communication, encryption, protection against tracking, anonymous browsing, etc. However, in many cases the functionality of such tools is not as expected, for example due to lack of transparency on the tool's development and operation or lack of proper maintenance mechanisms. Privacy enhancing technologies (PETs) that fail to offer what they promise can be very dangerous, as the false sense of protection can compromise the users' personal data and negatively affect or even out in harm's way their personal life.

Against this background, ENISA has been engaged over the last years in the development and practical implementation of a systematic approach for the assessment and presentation of online privacy tools for the general public (the PETs control matrix). Starting from the aforementioned work, the scope of this panel is to examine the availability of reliable online privacy tools today, the information that is provided to end users, the potential of self-assessment of privacy tools (by PETs developers), as well as the level of awareness of web and mobile users on PETs.

2.2.2 Appropriate security measures for the processing of personal data

Information risk management is an integral part of an organization's management process that deals with the identification, treatment, communication and acceptance of IT security risks. It involves the selection and implementation of measures justified by the identified risks and the reduction of those risks to acceptable levels. It also comprises continuous monitoring of risks and risk communication. Several methodologies and frameworks have been proposed and have been adopted by organizations during the last decade but none of them was oriented on the protection of personal data.

Under the European legal framework, personal data can only be collected under specific conditions, for a legitimate purpose. Furthermore, organisations which collect, process and store personal data must protect it from misuse and they are obliged to ensure that technical and organisational measures are undertaken so as to protect the personal data with an appropriate level of security. Data subjects should have the same level of protection, regardless of the size of the organisation or the amount of personal data it processes. In 2014, Article 29 Data Protection Working Party has acknowledged that this protection can be done on in a scalable manner and has issued a statement on the role of a risk-based approach in data protection legal frameworks.

Such a risk-based approach should enable organizations to identify and assess the risks, likelihood and impact, and prioritize the events that could compromise the integrity and confidentiality of personal data. Following the risk assessment, it should also support organizations to select appropriate security and organizational measures and control to mitigate the identified risks, the potential impact and reduce the probability of occurrence.

2.2.3 Developing and maintaining a PET maturity repository

In recent years ENISA contributed to the definition of privacy and security by design, i.e. answering the question what the practical implications of these terms are. In the course of this work, ENISA developed a methodology that allows to compare different Privacy Enhancing Technologies (PETs) with regard to their maturity, i.e., their technology readiness and their quality concerning the provided privacy notion. This methodology was turned into a structured process and a community tool was developed.

The panel presented this tool for the first time to a wider expert public. Further, we discussed possibilities on how such a repository can be build and maintained

2.3 Scientific track

As in previous years, half of the conference agenda was dedicated to presentations of new ideas from research. To identify these new ideas, a call for papers was published in February 2016. This call was advertised by the programme committee (PC) members and published at relevant platforms, e.g. wiki-CfP[2]. The PC presented in section A.1.2 was composed of 50 senior academics, about 30% legal and 70% technical experts (computer science, electrical engineering). The review was single blind (reviewer knew authors, but authors did not know their reviewer) and a conflict of interest policy was enforced: a CoI was considered if reviewer and author were 1) academic siblings, 2) co-authors in the last 2 years or 3) in economic dependency from each other. The submission process was supported by EasyChair[3].

We received 32 submissions in response to our call for papers, see appendix. Each paper was peer-reviewed by at least four members of the international programme committee. Based on significance, novelty and scientific quality, we selected six full research papers. In order to support less experienced researchers, an additional seven papers were selected to undergo shepherding, i.e. a PC member was in close contact with the authors advising how to improve the paper. Six papers of those seven eventually met our quality standards and accepted for presentation and publication.

The first session, eIDAS and Data Protection regulation, discussed topics concerning data life cycle agreements, processes for privacy impact assessment and electronic IDs in a policy and organizational context. The second session, IoT and Public Clouds, discussed privacy and legal aspects in IoT, Cloud computing and their associated technological domains. Finally, the third session, Privacy Policies and Privacy Risk Representation, took the user on board, discussing privacy indicators to better communicate to users privacy policies and potential privacy risks. The proceedings, LNCS 9857, are available online.

[2] http://www.wikicfp.com/cfp/
[3] http://easychair.org/

3. Cooperation agreement and other practical arrangements

As legal basis, we set up a cooperation agreement with the local co-organizer, which essentially stated that ENISA will cover loses of the local co-organizer up to 20k. Cost above this limit need to be covered by fees and sponsorships.

The conference fee was set at euro 400, and discounted for early bird registration to Euro 250 and Euro 200 for students.

This year's search for sponsors was less successful than other years. We acquired 2 sponsors: one trust and the USEMP project, both contributing up to Euro 2000. The fact that we signed a MoU with f-secure was an inhibiting factor for other sponsors, thus we would expect more success in the following years.

Over all, with planning well in advance, we would expect that APF could be transformed into a self-sustaining event, with costs covered by fees and sponsorship.

4. Conclusion and Recommendations

In conclusion, the 4th incarnation of the annual privacy forum was a full success. Nevertheless, there is always room for improvement. Hence, we recommend for future APF

- **Early planning.** is crucial for call for papers, keynotes and advertisement. The next conference and local organiser should be announced at closure of the event, the *call for papers* should be online not later than 10 month before the event. Hence, best-suited project life cycle is about *13 months*, with early partnerships set between European institutions, local organisers and sponsors. We strongly advice *multiannual planning*.
- **Keep the CfP.** The paper track makes the event more interesting for industry participants. From their feedback, we know that they come for two reasons. Firstly to meet the policy makers and secondly to hunt for new talent.
- **Multi-disciplinary approach.** Compared to earlier APFs, in 2016 the APF was reaching out to industry (key notes) and to the legal community (30% of PC from law schools). However, there is still room for improvement. A stronger involvement of others discipline needs to be encouraged. We advise to invite a legal expert to the PC chair and to consider cooperating with other agencies, e.g. FRA.
- **Financial model.** APF could become self-sustainable. It would be recommendable to explore how sponsors could be better involved.
- **Location.** A co-organizer with its own conference facilities is highly recommendable.
- **Date.** The conference date needs to be selected careful. Especial competing events such as ESORICS, PETS, INFO Hiding need to be considered.

Annex A: Example of Annex

A.1 Call for Papers

A.1.1 Call text

Nowadays electronic communication networks and digital services are an essential part of an increasing number of everyday commodities. In the era of automated profiling and electronic surveillance, citizens face a serious threat against their right to privacy and informational self-determination, especially when using the internet and mobile services. The lack of transparency regarding the functionality and interconnection of such services increases the risk of uncontrollable processing of personal data. In this regard, the upcoming Data Protection Regulation will be a useful instrument to protect the privacy of individuals. However, for its successful implementation, this new framework needs to be enforced by proper technologies and encompassed with sustainable business models along with mechanisms to promote privacy awareness and help users to understand the value of their data.

The 2016 edition of the annual privacy forum is organized in the light of the upcoming data protection regulation and the European digital agenda. We invite papers covering original work on the technological, economic, legal and societal aspects of the challenges that will come up with the implementation of the new framework. We particularly invite multidisciplinary papers that make it explicit how the presented work can contribute to bridging the gap between research and policy.

To encourage contributions from policy makers, representatives of competent authorities (such as Data Protection Authorities), industry experts, NGOs, and civil society associations, we also invite opinion papers from all stakeholders on the above mentioned topics. Opinion papers will reflect the opinion/position of the author(s) on the selected privacy-related topic.

- Implementation aspects of ‘by design’ and 'by default' paradigms
- Implementation and adoption of PETs in today’s digital services
- Modelling of data protection and privacy requirements, such as: machine readable representations and automatic evaluation of policies
- Enabling transparency: technological and organizational challenges.
- Technical solutions for the enforcement and the implications of the subject’s right, e.g. right to erasure, access and correction.
- Aspects of privacy impact and risk assessment
- Technical solutions for data portability
- Sustainable business models for privacy friendly online services
- Information and consent in online environments: practical solutions and implementations
- Privacy awareness, reliability and usability of PETs
- Trust services for the protection of personal data - privacy aware trust services (i.e. electronic certificates, signatures, etc.)
- Security measures for the protection of personal data
- Economics of privacy and personal data

All submissions will be thoroughly reviewed by our PC members. We aim at minimal 3 average 4 reviews per paper. Furthermore, papers will be published in the proceedings of the conference, which will appear in Springer’s LNCS series

A.1.2 Programme Committee

General Co chairs

Prof. Dr. Kai Rannenberg, Goethe University Frankfurt
Dr. Demosthenes Ikonomou, ENISA, Athens

Scientific Program Committee Chairs

Dr. Jetzabel Serna, Goethe University Frankfurt
Dr. Stefan Schiffner ENISA, Athens

Program Committee

Sven Wohlgemuth, Independent Consultant
Bernhard C. Witt, it.sec GmbH & Co. KG
Diane Whitehouse, IFIP working group 9.2 on social accountability and ICT
Andreas Westfeld, HTW Dresden
Stefan Weiss, Swiss Re
Jozef Vyskoc, VaF
Carmela Troncoso, IMDEA Software Institute
Morton Swimmer, Trend Micro
Jan Schallaböck, iRights.Law
Angela Sasse, UCL
Kazue Sako, NEC
Heiko Roßnagel, Fraunhofer IAO
Vincent Rijmen, KU Leuven
Charles Raab, University of Edinburgh
Christian W. Probst, Technical University of Denmark
Joachim Posegga, University of Passau
Siani Pearson, HP Labs
Aljosa Pasic, Atos Origin
Peter Parycek Danube, University Krems
Sebastian Pape, Goethe University Frankfurt
Jakob Illeborg Pagter, Alexandra Institute
Gregory Neven, IBM Research
Chris Mitchell, Royal Holloway University of London
Vashek Matyas, Masaryk University
Fabio Martinelli, IIT-CNR
Daniel Le Métayer, INRIA
Gwendal Le Grand, CNIL
Stefan Köpsell, TU Dresden
Sabrina Kirrane, WU Wien
Els Kindt KU, Leuven
Dogan Kesdogan, University of Regensburg
Florian Kerschbaum, SAP
Stefan Katzenbeisser, TU Darmstadt
Sokratis Katsikas, NTNU
Marko Hölbl, University of Maribor
Marit Hansen, ULD Schleswig-Holstein

Lorena González Manzano, Universidad Carlos III de Madrid
Simone Fischer-Hübner, Karlstad University
Mathias Fischer, University of Muenster
Hannes Federrath, University of Hamburg
Thomas Engel, University Luxembourg
Prokopios Drogkaris, ENISA
Josep Domingo-Ferrer, Universitat Rovira i Virgili
Roberto Di Pietro, Bell Labs
José María De Fuentes, Universidad Carlos III de Madrid
Malcolm Crompton, IIS
Fanny Coudert, KU Leuven
George Christou, University of Warwick
Claude Castelluccia, INRIA Rhone-Alpes
Valentina Casola, UNINA
Pompeu Casanovas, UAB
Bettina Berendt, KU Leuven
Luis Antunes, University of Porto

A.2 Programme

Day 1. Wednesday, September 07, 2016	
8:30	Registration & Coffee
9:00	**Opening Ceremonies** Manfred Schubert-Zsilavecz, VP, Goethe University Frankfurt, Udo Helmbrecht, ED, ENISA, Wojciech Wiewiórowski, EDPS
9:15	**Opening Keynote: Data Protection in the Digital World** Thomas Kremer, Deutsche Telekom, Board member for Data Privacy, Legal Affairs and Compliance
10:15	Coffee
10:45	**Paper Session: eIDAS and Data Protection Regulation** ▪ ***A Lifecycle for Data Sharing Agreements: How it works out*** **José Francisco Ruiz** and Anil Ozdeniz, Atos Marinella Petrocchi, Ilaria Matteucci and Gianpiero Costantino, Institute of Informatics and Telematics (IIT) CNR Carmela Gambardella and Mirko Manea, Hewlett Packard Enterprise ▪ ***Process for Data Protection Impact Assessment under the European General Data Protection Regulation*** **Felix Bieker**, Marit Hansen, Hannah Obersteller and Martin Rost, ULD Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research (ISI) ▪ ***Bring your own Identity - Case Study from the Swiss Government*** **Gion Sialm**, Federal Office of Information Technology, Systems and Telecommunication FOITT Silvia Knittl, CSC Deutschland Consulting GmbH ▪ ***The E-Waste Privacy Challenge*** **Barbara Krumay,** Vienna University of Economics and Business
12:15	Lunch
13:30	***Panel I: Online Privacy Tools for the General Public*** ***Moderator: Athena Bourka, ENISA*** *Claude Castelluccia, INRIA* *Diego Naranjo, EDRI*

	Marit Hansen, ULD *Rolf Wendolsky, JonDos* We will focus on the available technologies, the type and reliability of information that is provided to end users, the potential of assessment (and comparison) of different tools, as well as the level of general user awareness on PETs.
14:45	Networking Coffee
15:15	**Paper Session: IoT and Public Clouds** ▪ ***Challenges of the Internet of Things: Possible Solutions from Data Protecy and 3DPrivacy*** **Luca Bolognini** and Camilla Bistolfi, Italian Institute for Privacy ▪ ***Smart Meters as non-Purpose Built Surveillance Tools*** **Jonida Milaj** and Jeanne Pia Mifsud Bonnici, University of Groningen ▪ ***Consumer Privacy on Distributed Energy Markets*** **Niklas Büscher**, Technische Universität Darmstadt. Stefan Schiffner, ENISA. Mathias Fischer, Universität Münster ▪ ***Selected Cloud Security Patterns to Improve End User Security and Privacy in Public Clouds presented*** **Thomas Länger** and Solange Ghernaouti, Swiss Cybersecurity Advisory and Research Group (SCARG). Henrich C. Pöhls, Passau Univ.
16:45	**State of the Net:** Mikko Hypponen, F-Secure, Chief Research Officer
19:00	Social Event and Signature ceremony for MoU between ENISA and F-Secure
Day 2. Thursday, September 08, 2016	
8:30	Registration & Coffee
9:00	**Paper Session: Privacy Policies and Privacy Risk Representation** ▪ ***PrivacyInsight: The Next Generation Privacy Dashboard*** **Christoph Bier**, Kay Kühne and Jürgen Beyerer, Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) ▪ ***A Framework for Major Stakeholders in Android Application Industry to Manage Privacy Policies of Android Apps*** **Shi-Cho Cha**, Tzu-Ching Liu, Sih-Cing Syu, Li-Da Chien and Tsung-Ying Tsai, National Taiwan University of Science and Technology. Chuang-Ming Shiung, Criminal Investigation Bureau Taiwan ▪ ***Qualitative Privacy Description Language - Integrating Privacy Concepts, Languages, and Technologies*** **Jasper van de Ven** and Frank Dylla, Bremen University ▪ ***An Information Privacy Risk Index for mHealth Apps presented by Thomas Brüggemann*** **Thomas Brüggemann** and Joel Hansen, University of Cologne. Tobias Dehling and Ali Sunyaev, University of Kassel
10:30	Coffee
10:45	***Panel II: Processing Personal Data*** ***Moderator: Prokopios Drogkaris, ENISA*** *Giuseppe D'Acquisto, Italian Data Protection Authority* *Fernando Pocas Da Silva, EU-LISA* *Oliver Grün, European Digital SME Alliance* *Marie Charlotte Roques Bonnet, Microsoft EMEA*
12:15	Lunch
13:30	***Panel III: Developing and maintaining a PETs maturity repository*** ***Moderator: Stefan Schiffner, ENISA*** *Meiko Jensen, FH Kiel, Wojciech Wiewiórowski, EDPS* *TBA, iTTi* *The panel will explore the possibilities of a community portal for maturity assessments. The prototype for the platform will be presented and its test run will be launched. Further, it will be discussed how to find a permanent host for such a platform.*

14:45	Coffee
15:00	**Closing Keynote: Observations on privacy and data protection from a security perspective** Jacoba Sieders, ABN AMRO, Global Head Identity & Access Management
15:45	End of Event

A.3 Budget break down

The final costs breakdown is being prepared by the local co-organisers.

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu