Annual Privacy Forum 2017

Annual Privacy Forum

BRINGING RESEARCH & POLICY TOGETHER

7-8 JUNE

UNIVERSITY OF VIENNA

VIENNA|AUSTRIA

The General Data Protection Regulation aims at reinforcing individuals' privacy in the digital era. How can technology be on its side? Join APF for a discussion on privacy engineering and technical solutions to data protection.

http://privacyforum.eu

enisa

European Commission

universität wien

WLAN: GuestNet
Passwort: gcogast1!

Table of contents

Welcome to APF2017 in Vienna!

It is our great pleasure to welcome you in Vienna for the 5th Annual Privacy Forum (APF), which will take place in Vienna, Austria, during June 7–8, 2017, organized by the European Union Agency for Network and Information Security, the European Commission Directorate General for Communications Networks, Content and Technology, and University of Vienna, as host. A very interesting programme is waiting for you!

Keynote speakers:

- Wojciech Wiewiórowski, EDPS
- Peter Fleischer, Google: Technology and Privacy: how Google is preparing for the GDPR
- Reinhard Posch, TU Graz & Austria Chief Information Officer: Data protection issues into the context of modern technology environments
- Rosa Barcelo, European Commission: ePrivacy Regulation proposal

Three paper sessions:

- "Data Protection Regulation", discusses topics concerning big genetic data, a privacy-preserving European identity ecosystem, the right to be forgotten und the re-use of privacy risk analysis;
- "Neutralisation and Anonymization", discusses neutralisation of threat actors, privacy by design data exchange between CSIRTs, differential privacy and database anonymization;
- "Privacy Policies in Practice", takes the user on board, discussing privacy by design, privacy scores, privacy data management in healthcare and trade-offs between privacy and utility.

Four panel sessions:

- "Privacy regulation in a global context considering new challenges like AI" – to examine privacy-friendly solutions for a global market with big data analytics allowing more personalised services;
- "Towards a European Data Protection Certification Scheme" – to explore the state of the art of certification mechanisms and data protection seals and marks;
- "Practical Implementation of GDPR in Mobile Applications" – to discuss the application of data protection obligations in the area of mobile applications;
- "Lawful interception and PETs" – to find practical solutions between privacy enhancing tools and crime prevention.

Pre-proceedings are already available; we thank Springer International Publishing for publishing the proceedings of APF2017 in the LNCS series.

APF 2017 would not have been possible without the commitment of many people around the globe volunteering their competence and time. We would therefore like to express our sincere thanks to the members of the PC – and to the authors who entrusted us with their works. Many thanks also go to our sponsors, in particular Microsoft, and to all conference attendees, who honoured the work of the authors and presenters. Last but not least, we would like to thank the Organizing Committee. Their excellent and tireless efforts made this event possible.

June 2017

Erich Schweighofer

Co-chair and Local chair, APF2017

APF2017

Annual Privacy Forum
Vienna, Austria, June 7-8, 2017

organised by

European Union Agency for Network and Information Security (ENISA)

European Commission Directorate for Communications Networks, Content and Technology (DG CONNECT)

University of Vienna

Sponsors and Organisers

Program Committee

Luis	Antunes	Computer Science Dep., University of Porto
Bojana	Belamy	CIPL
Bettina	Berendt	KU Leuven
Athena	Bourka	ENISA
Pompeu	Casanovas	Universitat Autònoma de Barcelona and La Trobe University
Valentina	Casola	University of Naples "Federico II"
George	Christou	University of Warwick, UK
Fanny	Coudert	Centre for IT and IP Law (CiTiP), KU Leuven
Malcolm	Crompton	Information Integrity Solutions Pty Ltd and CSIRO
José María	De Fuentes	Universidad Carlos III de Madrid
Paul	de Hert	LSTS, VUB Brussel
Roberto	Di Pietro	Bell Labs
Josep	Domingo-Ferrer	Universitat Rovira i Virgili
Prokopios	Drogkaris	ENISA
Hannes	Federrath	University of Hamburg
Mathias	Fischer	University of Hamburg
Lorena	González Manzano	Universidad Carlos III de Madrid
Graham	Greenleaf	UNSW
Marit	Hansen	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Dominik	Herrmann	University of Hamburg
Marko	Hölbl	University of Maribor, Faculty of Electrical Engineering and Computer Science
Walter	Hötzendorfer	Research Institute AG & Co KG, Vienna
Sokratis	Katsikas	Center for Cyber and Information Security, NTNU
Stefan	Katzenbeisser	TU Darmstadt
Dogan	Kesdogan	Universität Regensburg
Peter	Kieseberg	Kibosec GmbH
Els	Kindt	K.U.Leuven -ICRI
Sabrina	Kirrane	Vienna University of Economics and Business
Dariusz	Kloza	Vrije Universitet Brussel
Stefan	Köpsell	TU Dresden
Gwendal	Le Grand	CNIL
Daniel	Le Métayer	Inria, Université de Lyon
Herbert	Leitold	A-SIT
Fabio	Martinelli	IIT-CNR
Vashek	Matyas	Masaryk University & Red Hat Czech
Chris	Mitchell	Royal Holloway, University of London
Andreas	Mitrakas	ENISA
Gregory	Neven	IBM Research - Zurich
Sebastian	Pape	Goethe University Frankfurt
Peter	Parycek	Danube-University Krems
Aljosa	Pasic	Atos
Hans-Juergen	Pollirer	Secur-Data Betriebsberatungs-GmbH
Joachim	Posegga	University of Passau
Charles	Raab	University of Edinburgh
Kai	Rannenberg	Goethe University Frankfurt
Vincent	Rijmen	KU Leuven
Heiko	Roßnagel	Fraunhofer IAO
Kazue	Sako	NEC
Peter	Schartner	Universität Klagenfurt - System Security Group
Ingrid	Schaumueller-Bichl	University of Applied Sciences Upper Austria

Stefan	Schiffner	ENISA
Erich	Schweighofer	University of Vienna
Jetzabel	Serna	Goethe University Frankfurt
Florian	Skopik	AIT Austrian Institute of Technology
Christoph	Sorge	Saarland University
Morton	Swimmer	Trend Micro, Inc
Christof	Tschohl	Research Institute AG & Co KG, Vienna
Patrick	Van Eecke	University of Antwerp
Jozef	Vyskoc	VaF
Edgar	Weippl	SBA Research
Stefan	Weiss	Swiss Re
Diane	Whitehouse	IFIP working group 9.2 on social accountability and ICT
Bernhard C.	Witt	it.sec GmbH & Co. KG
Harald	Zwingelberg	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

General Co-chairs

Erich	Schweighofer	University of Vienna
Kai	Rannenberg	Goethe University Frankfurt

Program Co-chairs

Erich	Schweighofer	University of Vienna
Herbert	Leitold	A-SIT
Andreas	Mitrakas	ENISA
Kai	Rannenberg	Goethe University Frankfurt

Survival Guide – APF2017

Registration/Conference Office

Please register at the conference office. There you receive your conference folder and all further information.

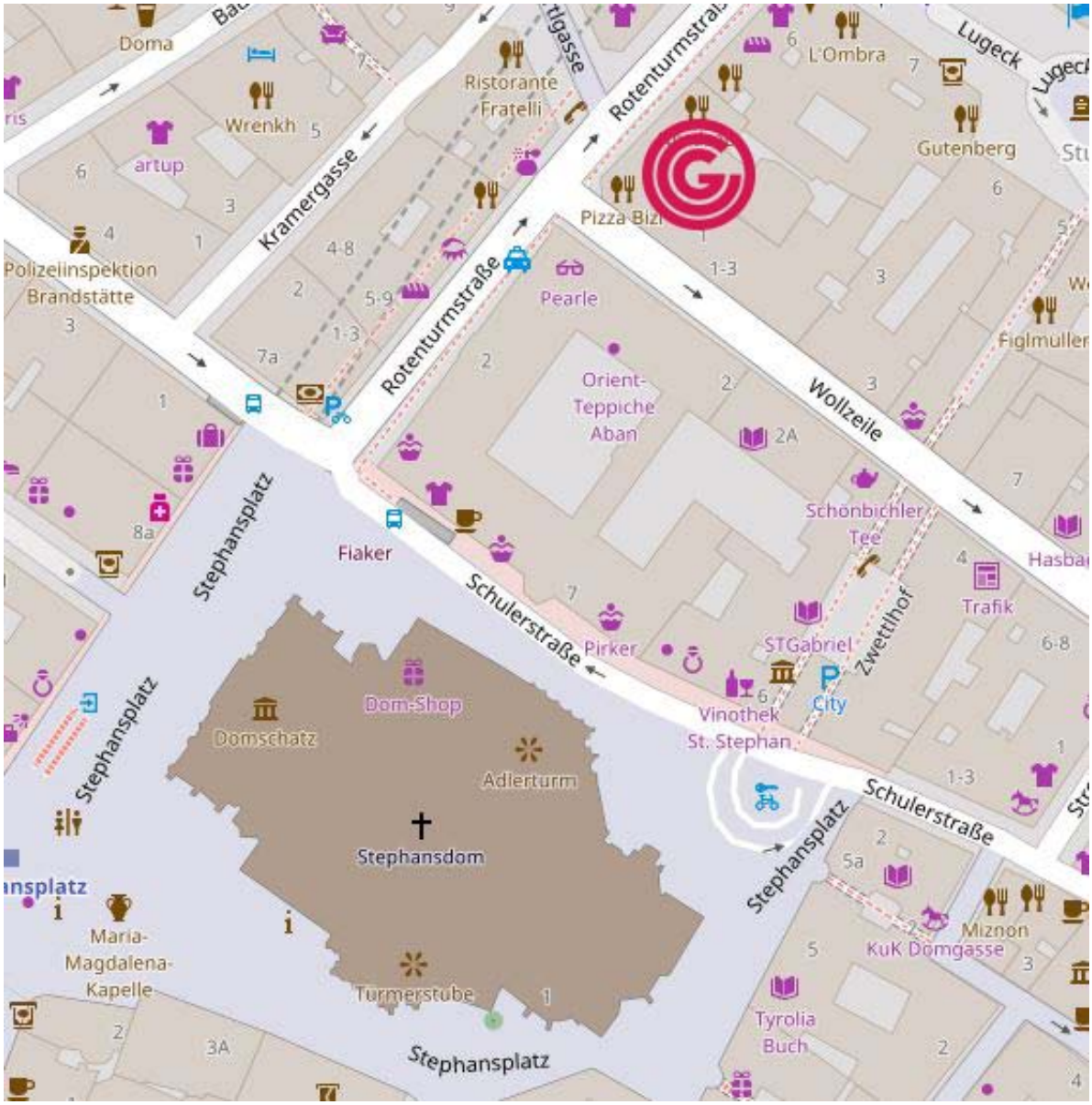
Conference Office
OCG Austrian Computer Society
Wollzeile 1, 1010 Wien
Mrs. Christine Hass
+43 1 5120235 51
Opening hours: Wednesday and Friday, 8.00-18.00
Please follow the signs!

Wi-Fi

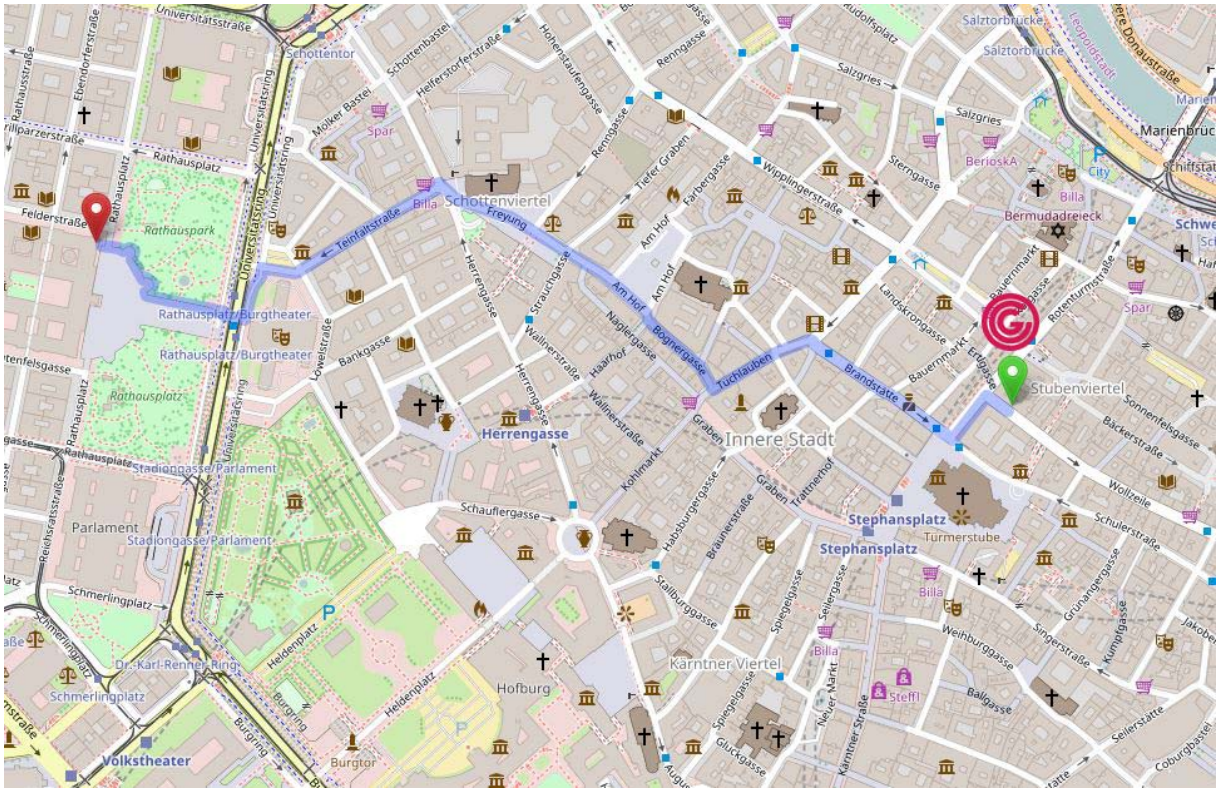
Maps

OCG Austrian Computing Society, Wollzeile 1, 1010 Wien

Very close to the St. Stephen's cathedral, the very heart of Vienna



Dinner at Rathauskeller, Rathausplatz 1, 1010 Wien



Further Information

Participation
Admission is subject to registration. Pre-registration online is necessary. Registration on-site is possible subject to availability.

Important Information
Because of fire safety regulations we need to know the number of participants. Therefore registration in the conference office is compulsory.

Name badge
Please return your name badge to the conference office before you leave the conference.

Copy service
You can make copies of hand-outs for your presentation in the conference office (at cost price). Please hand in your master document there early enough.

More …

- on the website: http://privacyforum.eu
- in the conference office.

Lunch

On Wednesday and Thursday a buffet lunch is offered at the conference site.

Evening Activities

Tuesday 6 June 2017, 6 p.m. Get2gether at OCG, Wollzeile 1, 1010 Wien

Wednesday: Dinner at City Hall – Rathauskeller, Rathausplatz 1, 1010 Wien (registration required!)

Local Organisation Team

University of Vienna: Erich Schweighofer, Vinzenz Heußler, Giti Said, Marta Banozic

OCG: Ronald Bieber, Christine Haas, Sandra Pillis

Programme of APF2017

As of 31 May 2017

ENISA Annual Privacy Forum, Vienna, Austria, June 7-8, 2017

Tuesday, 6 June 2017

Get2gether, 6 p.m., OCG, Wollzeile 1, 1010 Wien

Wednesday, 7 June 2017

Opening Remarks, 09:00-09:15

Paul Oberhammer, Dean of the Faculty of Law, University of Vienna
Erich Schweighofer, University of Vienna, Co-chair and local chair
Paulo Empadinhas, ENISA

Opening Keynotes, 09:15-10:30

Chaired by Erich Schweighofer, University of Vienna

Wojciech Wiewiórowski, EDPS
Peter Fleischer, Google: Technology and Privacy: how Google is preparing for the GDPR

Networking, coffee, tea, refreshments, air etc.: 10:30-11:00

Microsoft
Symantec
OneTrust
Privacy Management Software
Vision
Privacy Platform
NYMITY
innovating compliance
CREDENTIAL
universität
wien
OESTERREICHISCHE
COMPUTER GESELLSCHAFT
AUSTRIAN
COMPUTER SOCIETY
CEPIS
City of Vienna

Paper Session 1: Data Protection Regulation, 11:00-12:30

Chaired by Kai Rannenberg, Goethe University Frankfurt

Kärt Pormeister, The GDPR and Big Data: leading the way for Big Genetic Data?

Genetic data as a category of personal data creates a number of challenges to the traditional understanding of personal data and the rules regarding personal data processing. Although the peculiarities of and heightened risks regarding genetic data processing were recognized long before the data protection reform in the EU, the General Data Protection Regulation (GDPR) seems to pay no regard to this. Furthermore, the GDPR will create more legal grounds for (sensitive) personal data (incl. genetic data) processing whilst restricting data subjects' means of control over their personal data. One of the reasons for this is that, amongst other aims, the personal data reform served to promote big data business in the EU. The substantive clauses of the GDPR concerning big data, however, do not differentiate between the types of personal data being processed. Hence, like all other categories of personal data, genetic data is subject to the big data clauses of the GDPR as well; thus leading to the question whether the GDPR is creating a pathway for 'big genetic data'. This paper aims to analyse the implications that the role of the GDPR as a big data enabler bears on genetic data processing and the respective rights of the data subject.

Jorge Bernal Bernabe, Antonio Skarmeta Gomez, Nicolás Notario, Julien Bringer and Martin David, Towards a Privacy-preserving Reliable European Identity Ecosystem

This paper introduces the ARIES identity ecosystem aimed at setting up a reliable identity framework comprising new technologies, processes and security features that ensure highest levels of quality in secure credentials for highly secure and privacy-respecting physical and digital identity management processes. The identity ecosystem is being devised in the scope of ARIES European project and aspires to tangi- bly achieve a reduction in levels of identity fraud, theft, wrong identity and associated crimes and to create a decisive competitive advantage for Europe at a global level.

Beata Sobkow, Forget Me, Forget Me Not - Redefining the Boundaries of the Right to be Forgotten to Address Current Problems and Areas of Criticism

In the landmark decision *Google Spain v AEPD and Mario Costeja González,* the Court of Justice of the European Union has declared that individuals have a so-called 'right to be forgotten', that is, the right to demand search engines to erase search results obtained through searches for their names. The ruling has been praised by many and seen as a welcome relief for individuals who were gradually losing all control over the private information stored about them online. However, because the court has failed to provide proper guidance as to the application and scope of the new right, the ruling has opened risks to freedom of expression and the right to receive and impart information as well as introduced questions as to the legitimacy, fairness and international scope of the delisting process. Taking a closer look at the problems currently surrounding the right to be forgotten, this paper will attempt to narrow down and define the scope of the application of the new right. In order to do so, it will first argue that personal information should be predominantly protected by reliance on existing laws rather than through the creation of an ambiguous right to delist search results. It will then advocate for a rejection of the court's broad formulation of the right to be forgotten and suggest that, in order to attain a fairer balance between the fundamental rights at stake, the right should be only permitted to apply in three, clearly defined and limited circumstances.

Microsoft is the productivity and platform company for the mobile-first, cloud-first world. Our mission is to empower every person and every organization on the planet to do more and achieve more. Since the company was founded in 1975, we have worked to achieve this mission by creating technology that transforms the way people work, play, and communicate. We develop and market software, services, hardware, and solutions that deliver new opportunities, greater productivity, and enhanced value to people's lives. Microsoft lights up digital work and digital life experiences in the most personal, intelligent, open and empowering ways. We do business throughout the world and have offices in more than 100 countries, including each of the EU28 countries.

Website

http://www.microsoft.com/about

Sourya Joyee De and Daniel Le Métayer, A Refinement Approach for the Reuse of Privacy Risk Analysis Results

The objective of this paper is to improve the cost effectiveness of privacy impact assessments through (1) a more systematic approach, (2) a better integration with privacy by design and (3) enhanced reusability. We present a three-tier process including a generic privacy risk analysis depending on the specifications of the system and two refinements based on the architecture and the deployment context respectively. We illustrate our approach with the design of a biometric access control system.

Lunch: 12:30-13:30

Panel Session I: Practical Implementation of GDPR in Mobile Applications, 13:30-15:00

Chaired by Athena Bourka, ENISA

The objective of this panel is to discuss the current software development practices and challenges specific to app developers with regard to the processing of personal data and explore the level of practical implementation of GDPR.

Panel:

Marit Hansen, Unabhängiges Landeszentrum für Datenschutz

Arndt Gerdes, Huawei Technologies

Representative from EDPS

Peter Fleischer, Google

Networking, coffee, tea, refreshments, air etc.: 15:00-15:30

Paper Session 2: Neutralisation and Anonymization, 15:30-17:00

Chaired by Herbert Leitold, A-SIT

Andreas Rieb, Tamara Gurschler and Ulrike Lechner, A Gamified Approach to explore Techniques of Neutralization of Threat Actors in Cybercrime

In the serious game "Operation Digital Chameleon" red and blue teams develop attack and defense strategies as part of an IT security Awareness training. This paper presents the game design and selected results from a structured evaluation of techniques of neutralization applied by cybercrime threat actors. Various motives and five neutralization techniques are identified in fifteen instances of "Operation Digital Chameleon". We argue that "Operation Digital Chameleon" is not only an instrument to raise IT security awareness but also a sensible method to explore techniques of neutralization in cybercrime.

Erich Schweighofer, Vinzenz Heußler and Peter Kieseberg, Privacy by Design Data Exchange between CSIRTs

Computer Security Incident Response Teams ('CSIRTs') may exchange personal data about incidents. A privacy by design solution can ensure the compliance with data protection law and the protection of trade secrets. An information platform of CSIRTs is proposed, where incidents are reported in encoded form. Without knowledge of other personal data, only the quantity, region and industry of the attacks can be read out. Additional data – primarily from own security incidents – can be used to calculate a similarity to other incidents.

Maurizio Naldi and Giuseppe D'Acquisto, Mr X vs. Mr Y: the emergence of externalities in differential privacy

The application of differential privacy requires the addition of Laplace noise, whose level must be measured out to achieve the desired level of privacy. However, the protection of the data concerning a Mr. X, i.e., its privacy level, also depends on the other data contained in the database: a negative externality is recognized. In this paper we show that an attack on Mr. X can be conducted by an oracle, by computing the likelihood ratio under two scenarios, where the database population is made of either independent or correlated entries. We show that the target Mr. X can be spotted, notwithstanding the addition of noise, when its position happens to be eccentric with respect to the bulk of the database population.

Paul Francis, Sebastian Probst Eide and Reinhard Munz, Diffix: High-Utility Database Anonymization

In spite of the tremendous privacy and liability benefits of anonymization, most shared data today is only pseudonymized. The reason is simple: there haven't been any anonymization technologies that are general purpose, easy to use, and preserve data quality. This paper presents the design of Diffix, a new approach to database anonymization that promises to break new ground in the utility/privacy trade-off. Diffix acts as an SQL proxy between the analyst and an unmodified live database. Diffix adds a minimal amount of noise to answers|Gaussian with a standard deviation of only two for counting queries|and places no limit on the number of queries an analyst may make. Diffix works with any type of data and configuration is simple and data-independent: the administrator does not need to consider the identifiability or sensitivity of the data itself. This paper presents a high-level but complete descrip- tion of Diffix. It motivates the design through examples of attacks and defenses, and provides some evidence for how Diffix can provide strong anonymity with such low noise levels.

Panel Session II: Towards a European Data Protection Certification Scheme, 17:00-18:30

Chaired by Prokopios Drogkaris, ENISA

The objective of this panel is to identify and explore the challenges and opportunities of personal data protection certification mechanisms, seals or marks focusing also on existing initiatives and voluntary schemes.

Panel:

Jelena Burnik, Slovenian DPA

Bojana Bellamy, CIPL

Sebastian Meissner, EuroPriSe

Irene Kamara, Tilburg University (TILT), Vrije Universiteit Brussel (LSTS)

José M. del Álamo, TRUESSEC.EU

Dinner in City Hall, Rathauskeller, Rathausplatz 1, 1010 Wien (about 15 minutes walk), 19:00-22:00

Welcome address: Kurt Stürzenbecher, Member of the Provincial Parliament of Vienna, on behalf of the Major and Governor of Vienna Michael Häupl

Dinner address: Matthias Schmidl, Deputy Head, Austrian Data Protection Authority

---

"OneTrust is the leading privacy management software platform used over 1,000 organizations globally to comply with data privacy regulations across sectors and jurisdictions, including the EU GDPR and Privacy Shield.

Our comprehensive, integrated, technology-based solutions include readiness and privacy impact assessments, data inventory and mapping, automated identity and data discovery, website scanning and EU cookie compliance, subject rights and consent management, incident reporting, and vendor risk management.

The OneTrust platform is pre-configured with templates and workflows that can be easily tailored via our point-and-click UI based on unique industry and organizational requirements. We make it easy for privacy teams to get started with OneTrust by giving them the flexibility to upgrade platform capabilities as their program matures, deploy in the cloud or on premise, and scale to support a growing network of privacy champions.

OneTrust is based in Atlanta, GA and London, UK with a team of local privacy and technology experts across North America, Asia, and Europe."

https://onetrust.com

Thursday, 8 June 2017

Keynotes, 09:00-10:30

Chaired by Kai Rannenberg, Goethe University Frankfurt

Reinhard Posch, TU Graz & Austria Chief Information Officer: Data Protection Issues into the Context of Modern Technology Environments

Rosa Barcelo, European Commission: ePrivacy Regulation Proposal

Networking, coffee, tea, refreshments, air etc.: 10:30-11:00

Panel Session III: Privacy Regulation in a Global Context Considering New Challenges like AI, 11:00-12:30

Chaired by Erich Schweighofer, University of Vienna

User interfaces - hardware and software - are produced for a global market. AI tools with big data analytics allow more personalized services, resulting in a competitive advantage for respective companies. Therefore, privacy regulation must face these challenges and take into account that the global market must focus on privacy-friendly solutions. Ethics can play a strong role in this direction.

Panel:

Caroline Goemans Dorny, INTERPOL

Zoltán Précsényi, Symantec

Niko Härting, HÄRTING Rechtsanwälte

Maximilian Schrems, Privacy Activist

Lunch: 12:30-13:30

Paper Session 3: Privacy Policies in Practice, 13:30-15:00

Chaired by Andreas Mitrakas, ENISA

Majed Alshammari and Andrew Simpson, Towards a Principled Approach for Engineering Privacy by Design

Privacy by Design has emerged as a proactive approach for embedding privacy into the early stages of the design of information and communication technologies, but it is no `silver bullet'. Challenges involved in engineering Privacy by Design include a lack of holistic and systematic methodologies that address the complexity and variability of privacy issues and support the translation of its principles into engineering activities. A consequence is that its principles are given at a high level of abstraction without accompanying tools and guidelines to address these challenges. We analyse three privacy requirements engineering methods from which we derive a set of criteria that aid in identifying data-processing activities that may lead to privacy violations and harms and also aid in specifying appropriate design decisions. We also present principles for engineering Privacy by Design that can be developed upon these criteria. Based on these, we outline some preliminary thoughts on the form of a principled framework

that addresses the plurality and contextuality of privacy issues and supports the translation of the principles of Privacy by Design into engineering activities.

Max Maaß and Dominik Herrmann, PrivacyScore: Improving Privacy and Security via Crowd-Sourced Benchmarks of Websites

Website owners make conscious and unconscious decisions that affect their users, potentially exposing them to privacy and security risks in the process. In this paper we introduce PrivacyScore, an automated website scanning portal that allows anyone to benchmark security and privacy features of multiple websites. In contrast to existing projects, the checks implemented in PrivacyScore cover a wider range of potential privacy and security issues. Furthermore, users can control the ranking and analysis methodology. Therefore, PrivacyScore can also be used by data protection authorities to perform regularly scheduled compliance checks. In the long term we hope that the transparency resulting from the published benchmarks creates an incentive for website owners to improve their sites. We plan to announce the public availability of a first version of PrivacyScore at the Annual Privacy Forum in June 2017.

Vasiliki Diamantopoulou, Konstantinos Angelopoulos, Julian Flake, Andrea Praitano, José Francisco Ruiz, Jan Jürjens, Michalis Pavlidis, Dimitri Bonutto, Andrès Castillo Sanz, Haralambos Mouratidis, Javier García Robles and Alberto Eugenio Tozzi, Privacy Data Management and Awareness for Public Administrations: a Case Study from the Healthcare Domain

Development of Information Systems that ensure privacy is a challenging task that spans various fields such as technology, law and policy. Reports of recent privacy infringements indicate that we are far from not only achieving privacy but also from applying Privacy by Design principles. This is due to lack of holistic methods and tools which should enable to understand privacy issues, incorporate appropriate privacy controls during design-time and create and enforce a privacy policy during run-time. To address these issues, we present VisiOn Privacy Platform which provides holistic privacy management throughout the whole information system lifecycle. It contains a privacy aware process that is supported by a software platform and enables Data Controllers to ensure privacy and Data Subjects to gain control of their data, by participating in the privacy policy formulation. A case study from the healthcare domain is used to demonstrate the platform's benefits.

Bettina Berendt, Better Data Protection by Design through Multicriteria Decision Making: On False Tradeoffs between Privacy and Utility

Data Protection by Design (DPbD, also known as Privacy by Design) has received much attention in recent years as a method for building data protection into IT systems from the start. In the EU, DPbD will become mandatory from 2018 onwards under the GDPR. In earlier work, we emphasized the multidisciplinary nature of DPbD. The present paper builds on this to argue that DPbD also needs a multicriteria approach that goes beyond the traditional focus on (data) privacy (even if understood in its multiple meanings).

The paper is based on the results of a survey (n=101) among employees of a large institution concerning the introduction of technology that tracks some of their behaviour. Even though a substantial portion of respondents are security/privacy researchers, concerns revolved strongly around social consequences of the technology change, usability issues, and transparency. The results taken together indicate that the decrease in privacy through data collection was associated with (a) an increase in accountability, (b) the blocking of non-authorized uses of resources, (c) a decrease in usability, (d) an altered perception of a communal space, (e) altered actions in the communal space, and (f) an increased salience of how decisions are made and communicated. These results call into question the models from computer science / data mining that posit a privacy-utility tradeoff. Instead, this paper argues, multicriteria notions of utility are needed, and this leads to design spaces in which less privacy may be associated with less utility rather than be compensated for by more utility, as the standard tradeoff models suggest. The paper concludes with an outlook on activities aimed at raising awareness and bringing the wider notion of DPbD into decision processes.

Networking, coffee, tea, refreshments, air etc.: 15:00-15:30

Panel Session IV: Lawful Interception and PETs, 15:30-17:00

Chaired by Stefan Schiffner, ENISA

The EC3-ENISA joint working group on encryption invites to discuss practical solutions for the conflict where cryptographic tools that are used to prevent crime are also used by criminals to engage in crime. We will reflect the state of the art in electronic criminal investigations and what types of new evidence can be used during the investigations.

Panel:

Philipp Amann, Europol EC3

Laurent Beslay, DG Joint Research Centre

Stephan Krenn, AIT

Closing Session, 17.00-17.15

Chaired by Erich Schweighofer, University of Vienna

Andreas Mitrakas, Closing Remarks

Site events

privacyhub.wien - Annual Privacy Forum – OCG, 18.00-20:00, OCG, Wollzeile 1

http://privacyhub.wien

Invited talk: *Max Maaß and Dominik Herrmann,* PrivacyScore (in German)

Friday, 9 June 2017

IPEN - Internet Privacy Engineering Network, 9:00-16:00, OCG, Wollzeile 1

https://edps.europa.eu/data-protection/ipen-internet-privacy-engineering-network_en

Microsoft

universität
wien

City of Vienna