

11<sup>th</sup> INTERNATIONAL CONFERENCE 24 25 26 JANUARY 2018 BRUSSELS, BELGIUM  
**COMPUTERS, PRIVACY & DATA PROTECTION 2018**  
**THE INTERNET OF BODIES**  
 WWW.CPDPCONFERENCES.ORG



UNIVERSITÀ  
DEGLI STUDI  
DI TORINO

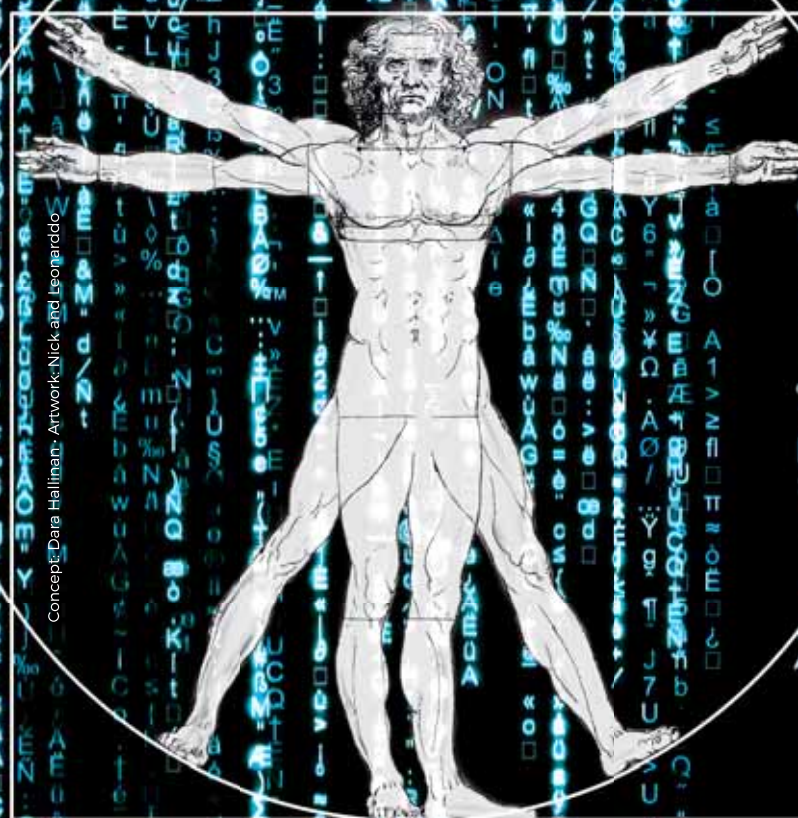


**CONTACT**

[www.facebook.com/CPDPconferencesBrussels](https://www.facebook.com/CPDPconferencesBrussels) [twitter.com/CPDPconferences](https://twitter.com/CPDPconferences) hashtag #CPDP2018

[info@cpdpconferences.org](mailto:info@cpdpconferences.org) [www.youtube.com/user/CPDPconferences](https://www.youtube.com/user/CPDPconferences)

11<sup>th</sup> INTERNATIONAL CONFERENCE  
 24 25 26 JANUARY 18 BRUSSELS, BELGIUM  
**COMPUTERS, PRIVACY  
 & DATA PROTECTION**  
**THE INTERNET  
 OF BODIES**



Concept: Dara Hallinan. Artwork: Nick and Leonardo

## FOREWORD

---

Dear participants of CPDP, dear colleagues, dear friends,

I am very happy to welcome you to Brussels, the data protection capital of Europe, for the 11th edition of CPDP! I hope many of you have already enjoyed our pre-events including Privacy Camp, GDPR Salon and the CPDP launch event on cross-border data transfers.

This year's overarching theme is the Internet of Bodies, paving the way for a timely and thorough discussion over a broad range of ethical, legal and policy issues related to new technologies that impact the body.

2018 will be known as the year that the GDPR came into force. What implications will the implementation of the GDPR have for companies, organisations and governments? I look forward to stimulating discussions about this topic. Our conference program promises to provide many more engaging discussions with topics ranging from e-privacy, e-evidence, encryption, cybersecurity to artificial intelligence, blockchain, data protection by design, gendered bodies, biometrics and more.

As usual, CPDP will take place in two venues — Les Halles de Schaerbeek and a new location for 2018, Area42. The new venue is only a short walk from Les Halles and lunch and coffeekbreaks will be organised in both venues.

Apart from the exciting CPDP panels during the day, there are numerous public side events happening in the evening, which includes Privacy Salons' second edition of **Privacytopia** including the art exhibition **Watching Me Watching You** at Bozar, a debate on cybersecurity at deBuren, an art exhibition **Painted by Numbers** in Area42 and the Glass Room Experience at Muntpunt.

I look forward to meeting many new faces and old friends and hope all of you will enjoy our conference!

Warm wishes,



Paul De Hert

11<sup>th</sup> INTERNATIONAL CONFERENCE  
24 25 26 JANUARY 18 📍 BRUSSELS, BELGIUM  
**COMPUTERS, PRIVACY  
& DATA PROTECTION**  
**THE INTERNET  
OF BODIES**

## CONTENTS

---

FOREWORD	3
GENERAL CONGRESS INFORMATION	7
<b>ORGANISATION OF CPDP2018</b>	<b>9</b>
CORE PROGRAMMING COMMITTEE	9
EXTENDED PROGRAMMING COMMITTEE	9
SCIENTIFIC COMMITTEE	9
MAP OF LES HALLES	11
RESTAURANTS CLOSE BY	11
CONFERENCE BOOKS	12
<b>AWARD CEREMONIES AT CPDP2018</b>	<b>13</b>
EPIC CHAMPION OF FREEDOM AWARD	13
EDPL YOUNG SCHOLARS AWARD	13
CNIL-INRIA AWARD	13

**CPDP2018 GRIDS**

**SEE SEPERATE BROCHURE**

## WEDNESDAY 24 JANUARY 2018

CPDP2018 PANELS AT GRANDE HALLE  
CPDP2018 PANELS AT PETITE HALLE  
CPDP2018 PANELS AT LA CAVE  
CPDP2018 PANELS AT AREA 42 GRAND  
CPDP2018 PANELS AT AREA 42 PETIT

## THURSDAY 25 JANUARY 2018

CPDP2018 PANELS AT GRANDE HALLE  
CPDP2018 PANELS AT PETITE HALLE  
CPDP2018 PANELS AT LA CAVE  
CPDP2018 PANELS AT AREA 42 GRAND  
CPDP2018 PANELS AT AREA 42 PETIT

## FRIDAY 26 JANUARY 2018

CPDP2018 PANELS AT GRANDE HALLE  
CPDP2018 PANELS AT PETITE HALLE  
CPDP2018 PANELS AT LA CAVE  
CPDP2018 PANELS AT AREA 42 GRAND  
CPDP2018 PANELS AT AREA 42 PETIT

## CPDP2018 SIDE EVENTS

WEDNESDAY 24 JANUARY 2018  
THURSDAY 25 JANUARY 2018  
FRIDAY 26 JANUARY 2018  
SATURDAY 27 JANUARY 2018

## EXHIBITIONS

## CPDP2018 SPONSORS LOGOS

## CPDP2018 SPONSORS

## CPDP2018 CONFERENCE PARTNERS

THANK YOU

14

14

17

20

24

28

31

31

34

37

43

46

49

49

52

55

58

61

63

64

65

66

66

67

39

69

76

75

## GENERAL CONGRESS INFORMATION

### INFORMATION DESK

We provide general information about the conference and inquiries about Brussels at the information desk in La Ruelle – located just inside the main entrance. For tourist information about Brussels please go to the VISIT- BRUSSEL concierge desk which is located in Le Village on the first day of the conference.

### INTERNET LOGIN AND PASSWORD

Login: CPDP · Password: CPDP2018

### AREA 42

Area 42 is our new venue this year. Two sessions will take place here: Area 42 Grand and Petit. Area 42 is located at 3 minutes walking distance (250 m) from Les Halles. Maps will be available at the information desk in La Ruelle. Students will be available on Wednesday to show the way to Area 42.

### LE VILLAGE @ LES HALLES & LOUNGE @ AREA 42

Welcome to Le Village (located in the Grande Halle) and Lounge @ Area 42 where you can meet your colleagues for networking during the coffee breaks and lunch and where the sponsor booths are located. The cocktail receptions take place in Le Village.

**During the sessions, Le Village/Lounge is closed (silent room!). The bar in La Ruelle and in Area 42 stays open for drinks (cash bar). Switch off your phone during all sessions please.**

### MEZZANINNE

On the Mezzanine (The Balcony) we provide a terrace where you can have your lunch or breaks. Entrance via the staircases in Le Village.

**During the sessions, the Mezzanine is a silent room! Switch off your phone or put it on silent mode during all sessions please.**

### NAME BADGE

You will receive a name badge with the dates of attendance. This is according to your registration. In case you would like to change your badge, please ask at the registration desk.

**Please ensure your badge is visible for the duration of the conference.**

### CHOOSE YOUR PRIVACY PREFERENCES AT CPDP 2018!

In your conference bag, you will find a set of four coloured buttons, called #offlinetags. By attaching one of these to your clothing, you can indicate what you want to be done with the photos of you possibly taken during the conference.



**Red** ('No photos, please') stands for the request not to take any photo of you.

**Blue** ('Blur me') expresses that you want your face to be made unrecognizable before uploading/sharing photos somewhere.

**Yellow** ('Don't tag') indicates that you are fine with photos being uploaded/shared but that you don't want these photos to be subject to name tagging or face recognition in order to prevent reverse searchability.

**Green** ('Upload me') finally stands for an acceptance of uploading, sharing, and tagging.

### POST-IT WALL

Do you have vacancies in your organization, would like to announce interesting meetings or projects or just want to share your ideas with all the conference participants? Post your information to our Post-It Wall, located in La Ruelle.

### TAXI

Please do not ask the information desk to call a taxi for you, please do this yourself. Companies like to know your name and phone number to avoid other people getting into the taxi you ordered. Taxi Verts T +32 2 349 49 49

### THE ANONYMIZER

We value your opinion! Your ideas, suggestions, remarks, etc. are welcome: Drop them in a dedicated box in at the registration desk in la Cave completely anonymously!

### UPDATES AND CONGRESS NEWS

Please find information at the registration desk, information desk and on the screens in the venue.

Alternatively, have a look at the CPDP home-page: [www.cdpconferences.org](http://www.cdpconferences.org) and our Attendify App which you can download from the App Store, Google Play. After downloading the app and creating a profile, you can join our CPDP 2018 event.



### VIDEO RECORDING

Is CPDP watching you? Well... a bit. You might be interested to know that all panels will be filmed at the Conference venue. Please check out our youtube channel: [www.youtube.com/user/CPDPConferences](https://www.youtube.com/user/CPDPConferences).

Please get in touch if you have any issues with this via [info@cpdpconferences.org](mailto:info@cpdpconferences.org) or mention this at the registration desk.

# Organisation of CPDP2018

- | Paul DE HERT (Vrije Universiteit Brussel LSTS, Tilburg University TILT), Director and Founder
- | Rosamunde VAN BRAKEL (Vrije Universiteit Brussel LSTS), Managing director
- | Dara HALLINAN (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure), Programme director

## CORE PROGRAMMING COMMITTEE

- | Paul DE HERT (Vrije Universiteit Brussel LSTS, Tilburg University TILT)
- | Rosamunde VAN BRAKEL (Vrije Universiteit Brussel LSTS)
- | Dara HALLINAN (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- | Imge OZCAN (Vrije Universiteit Brussel LSTS)
- | Lorenzo DALLA CORTE (Tilburg University TILT, TU Delft A+BE)
- | Diana DIMITROVA (FIZ Karlsruhe)

## EXTENDED PROGRAMMING COMMITTEE

- | Ronald LEENES (Tilburg University TILT)
- | Dennis HIRSCH (Ohio State University Moritz College of Law)
- | Malavika JAYARAM (Digital Asia Hub)
- | Omer TENE (International Association of Privacy Professionals)

## PANEL COORDINATORS

- | Yung Shin VAN DER SYPE (KU Leuven, time.lex)
- | Lina JASMONTAITE (Vrije Universiteit Brussel LSTS)
- | Irene KAMARA (Tilburg University TILT, Vrije Universiteit Brussel LSTS)
- | Ioulia KONSTANTINOOU (Vrije Universiteit Brussel LSTS)
- | Gianclaudio MALGIERI (Vrije Universiteit Brussel LSTS)
- | Deepan SARMA (Vrije Universiteit Brussel LSTS)
- | Barry GUIHEN (Vrije Universiteit Brussel LSTS)

## SCIENTIFIC COMMITTEE

- | Paul DE HERT (Vrije Universiteit Brussel LSTS, Tilburg University TILT)
- | Serge GUTWIRTH (Vrije Universiteit Brussel LSTS)
- | Rocco BELLANOVA (University of Amsterdam)

- | Franziska BOEHM (Karlsruhe Institute of Technology, FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- | Ian BROWN (UK Government Department for Digital, Culture, Media and Sport)
- | Willem DEBEUCKELAERE (Belgian Data Protection Authority)
- | Claudia DIAZ (Katholieke Universiteit Leuven ESAT)
- | Denis DUEZ (Université Saint-Louis - Bruxelles)
- | Michael FRIEDEWALD (Fraunhofer Institut für System- und Innovationsforschung ISI)
- | Marit HANSEN (Independent Centre for Privacy Protection, ULD)
- | Mireille HILDEBRANDT (Radboud Universiteit Nijmegen & Vrije Universiteit Brussel LSTS)
- | Dennis HIRSCH (Ohio State University Moritz College of Law)
- | Gus HOSEIN (Privacy International)
- | Kristina IRION (Marie Curie Fellow, Institute for Information Law IViR)
- | Els KINDT (Katholieke Universiteit Leuven Center for IT & IP Law)
- | Bert Jaap KOOPS (Tilburg University TILT)
- | Eleni KOSTA (Tilburg University TILT)
- | Ronald LEENES (Tilburg University TILT)
- | Daniel LE MÉTAYER (Institut National de Recherche en Informatique et en Automatique INRIA)
- | Charles RAAB (University of Edinburgh)
- | Marc ROTENBERG (Georgetown University Law Center)
- | Antoinette ROUVROY (University of Namur FUNDP, CRID)
- | Ivan SZEKELY (Eotvos Karoly Policy Institute, OSA Archivum)

## LOGISTICS AND REGISTRATION



Medicongress Services  
 Noorwegenstraat 49 · 9940 Evergem · Belgium  
 Phone: +32 (0)9 218 85 85  
[www.medicongress.com](http://www.medicongress.com) · [info@medicongress.com](mailto:info@medicongress.com)  
 Els VERTRIEST · Congress Manager  
 Laurence SCHEPENS · Assistant Congress Manager

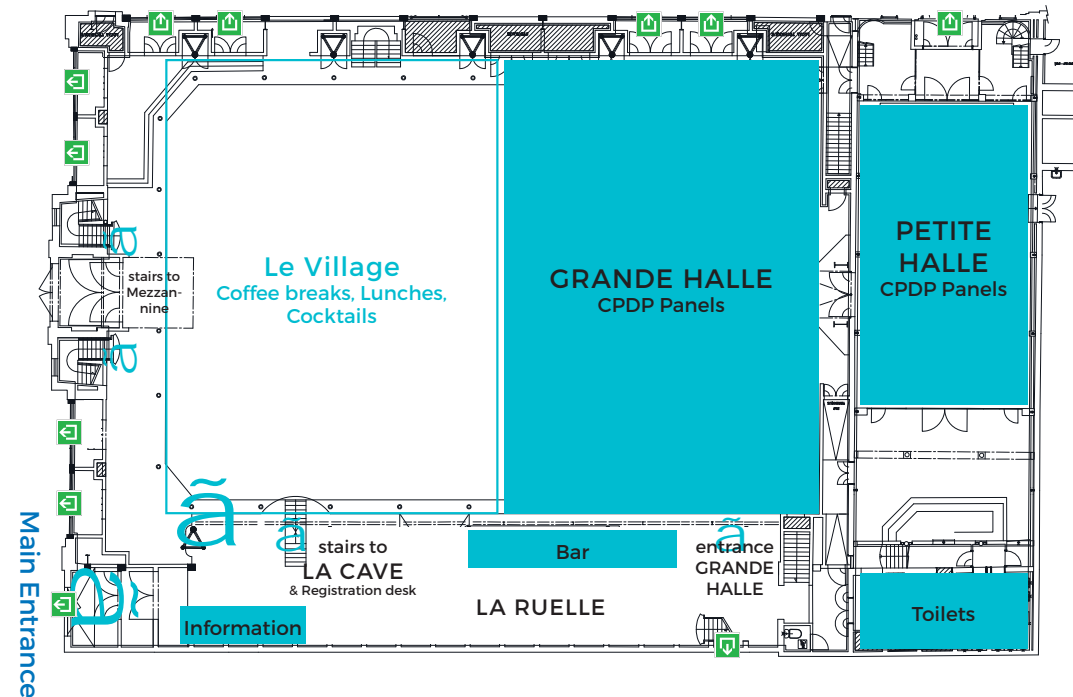
## LOGISTICAL AND ADMINISTRATIVE SUPPORT



Rosamunde VAN BRAKEL, Irina BARALIUC, Karin NEUKERMANS, Lore AERTS  
[www.privacysalon.org](http://www.privacysalon.org)

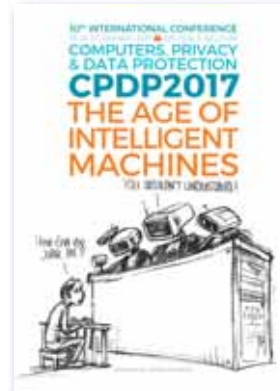
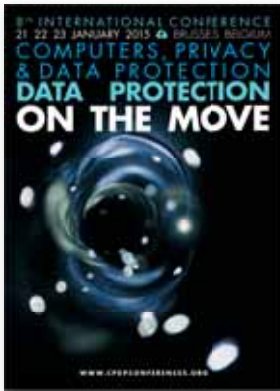
Design © Nick Van Hee – [www.nickvanhee.be](http://www.nickvanhee.be)

## LES HALLES



## RESTAURANTS CLOSE BY

- **Le Chambord** (Italian, Belgian) €€  
 Chaussée de Haecht 10 (close to Bloom)  
 +32 (0) 2 223 35 70  
 Open: 12:00 - 15:00 and 17:30 - 23:00
- **Brasserie De Groene Ezel** (Belgian) €€  
 Rue Royale Sainte Marie 11, 1030 Brussels  
 +32 (0)2 217 26 17  
 Open: 11.30-14.30 and 18.30-23.00
- **Le Millenium** (Italian) €€  
 Rue de Bériot 52 (not far from Bloom)  
 +32 (0) 2 223 03 55  
 Open 10.30-24.00
- **La Mamma** (Authentic Italian Food) €€€  
 Place Saint Josse 9, 1210 Brussels  
 +32 (0)2 230 53 00  
 Open: 12.00-16.00 and 18.30-23.30
- **Les Dames Tartine** (Old-Fashioned luxury) €€€  
 Chaussée de Haecht 58, 1210 Brussels  
 +32 (0)2 218 45 49  
 Open: lunch and supper
- **Café Bota** (inside Le Botanique) (Italian) €€  
 Rue Royale 236, 1210 Brussels  
 +32 (0)2 226 12 28  
 Open: 12-14.30 and 18.30-23.00



## CONFERENCE BOOKS

### Books based on papers presented at previous CPDP conferences:

- Gutwirth, S., Poulet, Y., De Hert, P., de Terwangne, C., and S. Nouwt, eds. **Reinventing Data Protection?** Dordrecht: Springer, 2009. ([www.springer.com/law/international/book/978-1-4020-9497-2](http://www.springer.com/law/international/book/978-1-4020-9497-2))
- Gutwirth, S., Poulet, Y., and P. De Hert, eds. **Data Protection in a Profiled World.** Dordrecht: Springer, 2010. ([www.springer.com/law/international/book/978-90-481-8864-2?changeHeader](http://www.springer.com/law/international/book/978-90-481-8864-2?changeHeader))
- Gutwirth, S., Poulet, Y., De Hert, P. and R. Leenes eds. **Computers, Privacy and Data Protection: an Element of Choice.** Dordrecht: Springer, 2011. ([www.springer.com/law/international/book/978-94-007-0640-8](http://www.springer.com/law/international/book/978-94-007-0640-8))
- Gutwirth, S., Leenes, R., De Hert, P. and Y. Poulet, **European Data Protection: In Good Health?** Dordrecht: Springer, 2012. ([www.springer.com/law/international/book/978-94-007-2902-5](http://www.springer.com/law/international/book/978-94-007-2902-5))
- Gutwirth, S., Leenes, R., De Hert, P. and Y. Poulet, **European Data Protection: Coming of Age** Dordrecht: Springer, 2012. ([www.springer.com/law/international/book/978-94-007-2902-5](http://www.springer.com/law/international/book/978-94-007-2902-5))
- Gutwirth, S., Leenes, R. and P. De Hert, **Reloading Data Protection.** Dordrecht: Springer, 2014. ([www.springer.com/law/international/book/978-94-007-7539-8](http://www.springer.com/law/international/book/978-94-007-7539-8))
- Gutwirth, S., Leenes, R. and P. De Hert, **Reforming European Data Protection Law.** Dordrecht: Springer, 2015 ([www.springer.com/law/international/book/978-94-017-9384-1](http://www.springer.com/law/international/book/978-94-017-9384-1))
- Gutwirth, S., Leenes, R. and P. De Hert, **Data Protection on the Move.** Dordrecht: Springer, 2016 ([www.springer.com/gp/book/9789401773751](http://www.springer.com/gp/book/9789401773751))
- Leenes, R., Van Brakel, R., Gutwirth, S., and P. De Hert, **Computers, Privacy and Data Protection: Invisibilities & Infrastructures.** Dordrecht: Springer, 2017 (<http://www.springer.com/gp/book/9783319507958>)
- Leenes, R., Van Brakel, R., Gutwirth, S. and P. De Hert, **Data Protection and Privacy: The Age of Intelligent Machines.** Oxford: Hart Publishing, 2017 (<https://www.bloomsburyprofessional.com/uk/data-protection-and-privacy-9781509919345/>)

# Award Ceremonies CPDP2018

## EPIC CHAMPION OF FREEDOM AWARD

The award is given annually to one individual outside of the United States who has shown great courage and dedication in the defense of privacy. Previous recipients of the award include Stefano Rodota (2009), Michael Kirby (2010), Sophie In't Veld (2011), Jennifer Stoddart (2012), Max Schrems (2013), Jan Philipp Albrecht (2014), Peter Hustinx (2015), Viviane Reding (2016) and Alexander Dix (2017).

The jury is chaired by Marc Rotenberg and consists of: Alessandro Acquisti, Ross Anderson, Colin J. Bennett, Simon Davies, David Flaherty, Pamela Jones Harbour, Paul De Hert, Kristina Irion, Malavika Jayaram, Pablo Molina, Helen Nissenbaum, Stephanie Perrin.

**Award ceremony Wednesday 24 January 2018 at 18.30 in Grande Halle**

## EDPL YOUNG SCHOLARS AWARD

The Young Scholars Award (YSA), hosted by the European Data Protection Law Review (EDPL) in cooperation with CPDP, is given annually to outstanding emerging researchers in the field of privacy and data protection law.

During this panel session, the three best young academics will present their research and discuss it with the competition jury members and the audience.

The winner of the award will be revealed at a ceremony at the end of the YSA panel.

Bart van der Sloot (Tilburg University), Maja Brkan (Maastricht University), and Mark Cole (University of Luxembourg) will discuss the papers. Serge Gutwirth (VUB) will award the prize.

**Award ceremony Thursday 25 January 2018 at 16.00 in Area42 - Petit**

## CNIL- INRIA PRIVACY AWARD

The CNIL-Inria Privacy Award is given annually to the authors of a computer science paper that contributes to the improvement of privacy or the protection of personal data. The paper may describe a fundamental research result, a technical innovation or provide a state of the art of a privacy related area. It must be the result of work carried out, at least in part, in a research lab in the European Union and must be published in the two years preceding the opening of the competition.

The jury is chaired by Daniel Le Métayer and consists of: Claude Castelluccia, Emiliano De Cristofaro, Josep Domingo-Ferrer, Simone Fischer-Hübner, Sébastien Gambs, Matthieu Grall, Krishna Gummadi, Jaap-Henk Hoepman, Gwendal Le Grand, Yves-Alexandre de Montjoye.

**Award ceremony Friday 26 January 2018 at 11.45 in Grande Halle**

# Wednesday 24 January 2018

## CPDP2018 PANELS AT GRANDE HALLE

### 8.30 - WELCOME AND INTRODUCTION BY PAUL DE HERT

### 8.45 - PHYSICAL TRACKING

**Academic • Policy • Business •**

**Organised by** INRIA

**Chair** Daniel Le Métayer, INRIA (FR)

**Moderator** Gloria González Fuster, VUB (BE)

**Speakers** Anna Fielder, Trans Atlantic Consumer Dialogue (UK), Mathieu Cunche, INSA Lyon (FR), Monica McDonnell, Informatica (UK), Jules Polonetsky, Future of Privacy Forum (US)

Tracking people in the physical world, through a variety of sensors, cameras, and mobile devices, is now common but it is becoming increasingly controversial. Knowing human dynamics such as crowd sizes, paths or visit durations are extremely valuable information for many applications. It offers great prospects to retailers or for urban planning. More generally, the extension to the physical world of the tracking already in place on the internet and the lack of control or even awareness of individuals raise serious questions. The goal of this panel is to discuss in a multidisciplinary way the issues raised by physical tracking, including the following questions:

- Is it possible to enhance individuals' control over their information (including information, consent and "do not track" options) in the context of physical tracking?
- What recommendations could be made regarding the ePrivacy Regulation and

the implementation of the GDPR to ensure better protection against physical tracking?

- Can self-regulation initiatives such as the Future of Privacy Forum code of conduct help improve the situation?

### 10:00 - Coffee break in Le Village

### 10.30 - THE INDIAN SUPREME COURT RULING AND ITS IMPLICATIONS FOR INTERNATIONAL DATA TRANSFERS

**Academic • Policy • Business •**

**Organised by** Intel

**Chair** Joseph Cannataci, UN Special Rapporteur on the Right to Privacy (INT)

**Moderator** Riccardo Masucci, Intel (BE)

**Speakers** (in Brussels) Malavika Jayaram, Digital Asia Hub (IN), Michael Donohue, OECD (INT), Bruno Gencarelli, DG Just (EU), (in Delhi) David Hoffman, Intel (US), Sudhanshu Pandey, Department of Commerce (IN), Rama Vedashree, Data Security Council of India (IN)

The recent Indian Supreme Court ruling on privacy opens up new scenarios both in India and internationally. This panel, in videoconference with a parallel session held in Delhi, aims to discuss citizens' rights in a data-rich environment, as well as explore the implications for global data flows in the context of EU adequacy decisions and future developments of the Schrems II case.

- What will the recognition of privacy as a fundamental right entail for current and

future data protection measures in India?

- What reforms should India embark on to be eligible for an adequacy decision by the European Commission?
- Which legal tools will be employed to ensure cross border data flows for Indian companies and for companies operating in India?

### 11:45 - GDPR IMPLEMENTATION: THE COUNTDOWN TO 25 MAY 2018

**Academic • Policy • Business •**

**Organised by** CPDP

**Chair** Fanny Hidvegi, Access Now (BE)

**Moderator** Cecila Bonefeld-Dahl, Digital Europe (BE)

**Speakers** Jan Albrecht, MEP (EU), Renate Nikolay, Cabinet of Commissioner Jourova (EU), Mark Cole, University of Luxembourg (LU), Eric Miraglia, Google (US)

The 25<sup>th</sup> of May 2018 - the date the General Data Protection Regulation (GDPR) will finally enter into force - is almost upon us. However there is still a lack of clarity as to what this date will bring. Despite its driving aim of harmonization, the GDPR still incorporates a number of opening clauses allowing Member States to choose whether and how its provisions apply - in relation to scientific processing for example. Despite its extensive nature, the GDPR still contains provisions whose substantive content remains vague and open to wide interpretation - Data Protection Impact Assessments for example. Despite its superficial stability, the GDPR foresees significant interpretative powers for both Member State and European level Data Protection Authorities - in relation to administrative fines for example. With just months left, the panel takes a look at implementation efforts to date, and considers where we go from here.

- What have key stakeholders done to implement the Regulation?
- Are there any problems with the results of these efforts?
- What remains to be done and what are the key obstacles preventing effective implementation moving forward?

### 13:00 - Lunch in Le Village

### 14:15 - BETWEEN TWO COMMISSIONS: VIEWS FROM DUBLIN AND BRUSSELS

**Academic • Policy • Business •**

**Organised by** IAPP

**Moderator** Omer Tene, IAPP (US)

**Speakers** Helen Dixon, Data Protection Commissioner (IE), Bruno Gencarelli, DG Just (EU)

With the 25 May 2018 implementation date looming, the European Commission is about to share responsibility for the implementation of the GDPR with national data protection commissioners in member states. Even with the statutory language in place, a margin of maneuver is left for national rules on certain issues ranging from professional secrecy to the age of consent. Meanwhile, the ePrivacy Regulation continues to make its way through the legislative process in Brussels and the Member States. The upcoming entry into application of the GDPR has also led to a renewed focus on adequacy decisions, with ongoing talks with Japan and South Korea. Against this backdrop, the CJEU is set to hear the case of Ireland's Data Protection Commissioner v. Facebook and Max Schrems, testing the validity of international data transfers based on European Commission approved standard contractual clauses and, possibly, the EU-US Privacy Shield. In this session, the Data Protection Commissioner of Ireland, a



global hub of the technology industry, discusses the policy, law and implementation of European data protection law with the head of the data flows and protection unit at the European Commission.

### 15:30 - Coffee break in Le Village

### 16:00 - TOWARDS A EUROPEAN PRODUCTION ORDER?

**Academic • Policy •**

**Organised by** Google

**Chair** Iain Mitchell, CCBE (BE)

**Moderator** Paul De Hert, VUB (BE)

**Speakers** Rita Balogh, Google (BE), Katalin Ligeti, University of Luxembourg (LU), Joe McNamee, EDRI (BE), Tania Schroeter, DG Just (EU)

For as long as we've had legal systems, prosecutors and the police have needed to gather evidence. And for each new advance in communications, law enforcement has adapted. The question the EU is facing now is how to support a new framework that allows such adaption to a rapid growth of technology, that address the very real security threats that people and communities face and which guarantees fundamental rights - such as the protection of private life. The Commission offers the European Production Order as a solution. Accordingly, the panel will discuss:

- How can EU level legislation address the challenges faced by law enforcement?
- What fundamental rights guarantees should this take into account?
- What global precedent do we hope to set?

### 17:15 - MOVING TOWARDS AN E-PRIVACY REGULATION

**Academic • Business • Policy •**

**Organised by** CPDP

**Chair** Joe McNamee, EDRI (BE)

**Moderator** Eleni Kosta, Tilburg University (BE)

**Speakers** Birgit Sippel, MEP (EU), Karolina Mojzesowicz, DG Just (EU), Rosa Barcelo, DG CNECT (EU), Joris van Hoboken, VUB (BE), Gary Davis, Apple (US)

The EU has paid special attention to privacy in electronic communications. In that regard it passed in 2002 the e-Privacy Directive as a lex specialis to the existing Data Protection Directive 95/46/EC (to be replaced by the GDPR). The dynamic technological developments have brought new challenges to the privacy of communications, e.g. new communication platforms. Thus, the EU legal framework was seen as unfit to ensure the confidentiality of present-day electronic communications. The GDPR raised the level of data protection, while also incorporating in its text several elements of the ePrivacy regulatory toolkit. The EU tabled at the beginning of 2016 a new legislative proposal for an e-Privacy Regulation with the aim of adapting the privacy rules to the new technological challenges. The panel will address the following questions related to the proposal:

- What challenges does the proposed e-Privacy Regulation seek to address?
- Is the Commission proposal ambitious enough? Are there loopholes?
- How does the proposal interplay with the GDPR?

### 18:30 - EPIC CHAMPION OF FREEDOM AWARD followed by Cocktail sponsored by EPIC in Le Village

## CPDP2018 PANELS AT PETITE HALLE

### 8.30 - WELCOME AND INTRODUCTION IN GRANDE HALLE

### 08:45 - TECHNICAL PROTECTION AGAINST ONLINE TRACKING AND PROFILING

**Academic • Policy • Business •**

**Organised by** ENISA

**Chair** Athena Bourka, ENISA (EU)

**Moderator** Kai Rannenbergh, Goethe University Frankfurt (DE)

**Speakers** Fenneke Buskermolen, DG CNECT (EU), Diego Naranjo, EDRI (BE), Mike O'Neill, BayCloud (UK), Rob van Eijk, Leiden University (NL)

While online users increasingly rely on smart connected devices (e.g. smartphones, Internet of Things devices) and relevant applications for their everyday activities and needs, the processing of personal data through such tools is not always transparent. Indeed, in many cases the processing results in users being tracked across different devices and applications, leading to extensive profiles, shared by different parties. How can technology support the adoption of protective measures in accordance with the underlying legal provisions of GDPR and the proposed ePrivacy Regulation? The panel will focus on discussing the state-of-the-art and gaps in the field, analyzing the way that technology can promote privacy and protection of personal data against online and mobile tracking and profiling.

- What are the main techniques for modern tracking in online and mobile environments?
- How can privacy by design support

against tracking?

- Are there any best practices for supporting tracking prevention and user consent?

### 10:00 - Coffee break in Le Village

### 10:30 - BLOCKCHAIN AND DATA PROTECTION: CHALLENGES AND OPPORTUNITIES

**Academic • Policy • Business •**

**Organised by** JRC

**Chair** Ricardo Neisse, JRC (EU)

**Moderator** Primavera De Filippi, CNRS (FR)

**Speakers** Sylvain Cariou, Crystalchain (FR), Jaap-Henk Hoepman, Radboud University (NL), Arnaud Le Hors, IBM (US), Gary Steri, JRC (EU)

Some of the fundamental characteristics of blockchains, such as immutability, auditability, and data replication can be seen as a challenge when data protection principles must be respected. This is especially challenging where anonymity assurances are bypassed if user transactions can be easily traced back to their initiator. Furthermore, immutability per se means transactions recorded cannot be erased without compromising the chronological integrity of the blockchain. Therefore, these technical aspects impose legal issues considering current EU regulations such as the GDPR. On the other hand, blockchains also have the potential to contribute to the implementation of these same regulations by adopting privacy enabling technologies. From these two perspectives, the aim of this session is to debate challenges and opportunities that the adoption of blockchain tech-

technologies may have with respect to legal data protection requirements. Considering the broad nature of the topic, the invited experts for this panel were selected to cover industry use cases and privacy issues from legal as well as technical perspectives.

- What are the fundamental benefits and limitations of blockchain technologies from a data protection perspective?
- What is the technical impact of data protection regulations on blockchain technologies?
- What are the technical/legal data protection challenges and opportunities foreseen on the large scale adoption of blockchain technologies?
- Can blockchains be used to empower citizens and, by embracing privacy enhancing technologies, contribute to enhancing the implementation of data protection?

#### 11:45 - EXPLORING THE “DESIGN” IN “PRIVACY BY DESIGN”

**Academic ... Policy .. Business ..**

**Organised by** Alexander von Humboldt Institute for Internet and Society (HIIG)

**Chair** Xuebing Zhou, Huawei (DE)

**Moderator** Max von Grafenstein, HIIG (DE)

**Speakers** Athena Bourka, ENISA (EU), Ame Elliott, Simply Secure (US), Jonathan Fox, Cisco (US), Katrin-Therese Lesny, Bundesdruckerei (DE), Harm van Beek, The Incredible Machine (NL)

Successful data-driven products are designed to be intuitive to use, but less user friendly when it comes to data protection and consent for disclosure. Why not design tomorrow's products in a way that makes the user's control of data protection risks as comfortable as the use of the product itself?

Articles 25 (and 32) of the upcoming EU GDPR require data controllers (and processors) to implement the „appropriate technical and organisational measures which are designed to implement data-protection principles“. However, what does the term „design“ in these requirements really mean? It seems highly valuable to redefine the term design not only as an addition but as a user-centric integral part of product and service development and usability. For the success of data protection and security measures the interdisciplinary panel will explore the concept of „design“ to highlight the importance of these questions:

- What is the legal meaning of the term “design” in “privacy and security-by-design”?
- Which role does the user play?
- What kind of design methodologies are appropriate, which best practices exist?

#### 13:00 - LAW ENFORCEMENT ACCESS TO E-EVIDENCE: CHALLENGES & RISKS

**Academic .. Policy .. Business ..**

**Organised by** Privacy Platform

**Chair and Moderator** Sophie In't Veld, MEP (EU)

**Speakers** Karsten Behn, Article 29 Working Party (EU), John Frank, Microsoft (BE), Estelle Massé, Access Now (EU)

The panel will discuss the recent developments concerning police access to evidence stored in other jurisdictions, such as the Microsoft search warrant case. With the increase of cloud computing, data that can be valuable in resolving criminal cases may be stored in data centres abroad. Considering that territoriality and sovereignty used to stop at the border, how can law enforcement authorities now get (legal) access to data across

the border, both between Member States and between the EU and third countries? What are the underlying challenges and risks for data protection? What is the role of tech companies? During the panel discussion this theme will be explored from a policy, legal, and tech perspective.

#### 14:15 - DATA PROTECTION BY DESIGN AND BY DEFAULT: SEMANTICS, RULES AND PROSPECTS

**Academic ... Policy .. Business ..**

**Organised by** Norwegian Research

Center for Computers and Law (NRCCL)

**Chair** Lee Bygrave, University of Oslo (NO)

**Moderator** Seda Gürses, KU Leuven (BE)

**Speakers** Marit Hansen, Data Protection Commissioner for Schleswig-Holstein (DE), Woodrow Hartzog, Northeastern University (US), Bert-Jaap Koops, Tilburg University (NL), Barbara Vieira, Software Improvement Group (NL)

This panel will assess the meaning and likely impact of the new requirements for data protection by design and by default in Article 25 of the General Data Protection Regulation. The panel will also place Article 25 in a broader historical, ideological and regulatory context, focusing particularly on its relationship with older notions of “privacy by design” and “privacy-enhancing technology”. Key questions for discussion are:

- What is the heritage of Article 25 and what does it essentially require?
- How may Article 25 be usefully operationalised?
- Are the requirements in Article 25 likely to gain any real traction in the systems development community?

#### 15:30 - Coffee break in Le Village

#### 16:00 - BODIES OF EVIDENCE: STRONG POINTS AND DRAWBACKS OF THE GDPR BETWEEN US AND EU

**Academic ... Policy ...**

**Organised by** University of Turin

**Chair** Shara Monteleone, European Parliament (EU)

**Moderator** Ugo Pagallo, University of Turin (IT)

**Speakers** Konstantinos Karachalios, IEEE (US), Argyro Karanasiou, Bournemouth University (UK), Alessandro Spina, EU EMA (EU), Marc Rotenberg, EPIC (US), Margot Kaminski, University of Colorado (US)

Crucial differences exist and persist between the US and EU regulations in the field of privacy and data protection. Yet, we could also say that such legal systems are separated by common goals. The aim of the panel is to shed further light on these differences and commonalities some weeks before the GDPR's direct applicability, by examining both the qualities and drawbacks of the new EU legal framework. Divergent judgements may of course hinge on different legal cultures. Still, diverse opinions may also depend on how we interpret some crucial rules and provisions of the GDPR: the latter can be understood either as a toothless mechanism or as a powerful means to safeguard the data subjects. The wording of the regulation allows either to be true. The following crucial issues come to the fore as a result:

- Will the GDPR amplify, or decrease, crucial differences between the US and EU regulations in the field of privacy and data protection?
- What are the strongest and weakest parts of the GDPR according to (also, but not only) a US viewpoint?

- What can the US legal system learn from the GDPR? Can GDPR alignment borrow from US best practices?

### 17:15 - DISCONNECTING FRAMEWORKS: E-PRIVACY, DIGITAL CONTENT DIRECTIVE AND THE GDPR

**Academic • Policy • Business •**

**Organised by** Privacy in Germany

**Chair** Olivier Micol, DG Just (EU)

**Moderator** Niko Härting, HÄRTING Rechtsanwälte (DE)

**Speakers** Bojana Bellamy, Hunton & Williams (UK), Damian Clifford, KU Leuven (BE), Gary Davis, Apple (IE), Helena Konig, Mastercard (NL), Sjoera Nas, Autoriteit Persoonsgegevens (NL), Axel Voss, MEP (EU)

The contents of legal frameworks for the connected world are disconnecting. This panel examines inconsistencies between the proposed ePrivacy Regulation, the Digital Content Directive and the GDPR.

One crucial aspect is the economic value of personal data. The Digital Content Directive proposes to recognise data as counter-performance and distinguishes between 'active' and 'passive' collection. This interferes with

the ePrivacy Directive and the GDPR's definition of personal data. The proposed ePrivacy regulation – e.g. through its failure to require default browser settings to be 'privacy-friendly' – seems inconsistent with the GDPR's requirements for consent and data protection by default. Another discrepancy between ePrivacy Regulation and GDPR is the recognition of 'legitimate interests' as a basis for data processing.

We will discuss the implications of those and other inconsistencies in the struggle for privacy and data protection. In doing so, we will analyse inherent conflicts in policy-making.

- The Digital Content Directive proposes to recognise data as counter-performance. Is this compatible with the GDPR paradigm?
- Is the proposed ePrivacy regulation consistent with the GDPR's requirements for consent and data protection by default?
- Will the ePrivacy Regulation need to recognise 'legitimate interests' as a basis for data processing following the GDPR?

### 18:30 - EPIC CHAMPION OF FREEDOM AWARD followed by Cocktail sponsored by EPIC in Le Village

**Academic • Policy • Business •**

**Organised by** AdLit Project

**Chair** Valerie Verdoodt, KU Leuven (BE)

**Moderator** Eva Lievens, Ghent University (BE)

**Speakers** Simone van der Hof, Leiden University (NL), Joëlle Jouret, Belgian

Privacy Commission (BE), Max Gersvang Sørensen, Lego Group (BE), Patrick Geary, UNICEF (INT)

Advertising has permeated the digital environments in which children play, communicate and search for information. The immersive, interactive and increasingly personalised nature of digital advertising techniques makes it difficult for children to recognise and make informed and well-balanced commercial decisions. Moreover, data mining and profiling of children's personal data for targeted advertising purposes raises important issues from a children's rights perspective (e.g. their right to privacy, right to development). The General Data Protection Regulation addresses some of these challenges by introducing specific protections for children, including inter alia the requirements for consent, age verification and profiling of children. However, it remains unclear how these provisions will be implemented in practice and how the provisions could complement children's advertising literacy and promote children's fundamental rights. For this panel we also draw on the fundamental legal research of the AdLit SBO project.

- How are children's rights reconfigured by digital advertising and marketing techniques, including inter alia their right to privacy, to play, to access to mass media sources and freedom of thought? Does a child's fundamental right to development or to education for example include a right to advertising literacy in this commercial context?
- How and to what extent does the GDPR aim to address the challenges posed by digital advertising techniques targeted at children in its provisions on the processing of children's personal data in light of the children's rights framework? Should there

for example be default limitations on data mining for advertising and marketing purposes?

- How are the abovementioned provisions implemented in practice and what kind of guidance on age verification, consent, profiling and use of children's personal data for commercial purposes do we have today? Which tools for age verification will for example be accepted under the GDPR and how will parental consent be organised practically? How does this compare to practices in the United States?
- What role is there for advertising literacy in light of children's (low) levels of understanding of advertising practices?

### 10:00 - Coffee break in Le Village

### 10:30 - MY DATA WAS COMPROMISED: HOW AM I SUPPOSED TO FIX IT? DATA BREACH NOTIFICATION AND PRIVACY

**Academic • Policy • Business •**

**Organised by** CANVAS project

**Chair** Esther Keymolen, Leiden University (NL)

**Moderator** Ailidh Callander, Privacy International (UK)

**Speakers** Susan Gonscherowski, Independent Centre for Privacy Protection Schleswig-Holstein (DE), Lina Jasmontaite, VUB (BE), Christian Wiese Svanberg, Danish National Police (DK), Christiaan Alberdingk Thijm, Bureau Brandeis (NL)

Personal data breaches have to be documented and in some cases notified by controllers to data protection authorities and individuals. In particular, the GDPR requires controllers to inform individuals whose data were subjected to a data breach about the likely consequences of the personal data breach and the measures taken or proposed

## CPDP2018 PANELS AT LA CAVE

### 8:30 - WELCOME AND INTRODUCTION IN GRANDE HALLE

### 8:45 - GROWING UP WITH ADVERTISING IN A DIGITAL MEDIA ENVIRONMENT: DATA PROTECTION SAFEGUARDS IN DISGUISE

to be taken by the controller to address the personal data breach. In preparation for the implementation of this new obligation in the EU, businesses organised many debates and even new business models have emerged. At the same time, the discussion about the actual impact on individuals' rights and actions that they could take after receiving a notification has been on halt.

- How to ensure that the obligatory reporting of security breaches facilitates protection of individuals' rights?
- How could one evaluate risk occurring to individuals from a data breach?
- How should damages be quantified in data breach claims?

#### 11:45 - PRIVACY ENGINEERING: LINGUA FRANCA FOR TRANSATLANTIC PRIVACY

**Academic • Policy • Business •**

**Organised by** Future of Privacy Forum

**Chair** Achim Klabunde, EDPS (EU)

**Moderator** Gabriela Zanfir-Fortuna, FPF (US)

**Speakers** Simon Hania, Tomtom (NL), Jeff Jonas, Senzing (US), Naomi Lefkowitz, NIST (US), Carmela Troncoso, École Polytechnique Fédérale de Lausanne (CH), Ari Ezra Waldman, New York Law School (US)

This panel will contribute to the essential transatlantic privacy debate by focusing on privacy engineering and the role it could play as "lingua franca" between the US and the EU privacy and data protection worlds. Privacy engineering is more important than ever in a time where accountability is significantly transferred to the creators of data centric systems. The state of the art of privacy engineering will be discussed with leading experts from the US and Europe, focusing on the latest solutions for embedding privacy safe-

guards in processing systems from their design stage, but also for quintessential issues such as de-identification, data portability, encryption, user control over data.

- How big of a role does privacy engineering have for enhancing privacy of individuals/users/consumers/digital citizens? Should it bear most of the "burden"? With whom else should privacy engineering share the "burden"?
- Could privacy engineering become a lingua franca of the US and EU privacy worlds? Is it already in this position?
- Is privacy by design achievable on a mass scale? Which are the factors that would facilitate the overall adoption of privacy by design?

#### 13:00 - Lunch in Le Village

#### 14:15 - NATIONAL IMPLEMENTATIONS OF THE GDPR: CHALLENGES, APPROACHES, STRATEGIES

**Academic • Policy • Business •**

**Organised by** Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe, for Forum Privacy and Self-Determined Life in the Digital World

**Chair** Michael Friedewald, Fraunhofer ISI (DE)

**Moderator** Walter van Holst, EDRI member Vrijschrift (NL)

**Speakers** Christian Geminn, University Kassel (DE), Karolina Mojzesowicz, DG Just (EU), Olivia Tambou, Université Paris-Dauphine (FR), Günther Leissler, Schoenherr Attorneys at Law (AT)

Though the GDPR was intended to "harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member

States" it provides a lot of leeway for Member States in its implementation, leaving significant room for derogations. This "margin of manoeuvre" creates the opportunity for the member states to specify vague concepts or to adapt the legal rules to the specific national context. There has been a vivid debate on how big the "margin of manoeuvre" actually is.

This panel asks how far Member States have actually progressed to adapt their national regulatory framework, what general approaches they have chosen to abolish or amend in existing data protection law, if they plan to make use of the opening clauses, how and why. The panel will also be asking about the rationale behind this activity and which issues are most intensively debated in this process. Finally the panel will discuss if the national implementation activities are likely to contribute to the harmonization process or if any new conflicts can be foreseen.

- Will the goal of European harmonization of data protection be reached or will national implementations lead to new fragmentation?
- How do different EU Member States approach the challenge of readying their national laws for the GDPR?
- What are the difficulties of implementing the GDPR within EU Member States?

#### 15:30 - Coffee break in Le Village

#### 16:00 - ANONYMOUS COMMUNICATIONS INFRASTRUCTURES FOR THE PROTECTION OF METADATA

**Academic • Policy • Business •**

**Organised by** PANORAMIX Project

**Chair** Aggelos Kiayias, University of Edinburgh (UK)

**Moderator** Claudia Diaz, KU Leuven (BE)

**Speakers** Gus Hosein, Privacy International

(UK), Moritz Bartl, Renewable Freedom Foundation (DE), Carmela Troncoso, EPFL (CH), Eleni Kosta, Tilburg University (NL)

Anonymous communication infrastructures are a key building block for the protection of online privacy. While the last years have seen a dramatic increase in the integration of end-to-end encryption for the protection of communications content, the protection of metadata has received far less attention, with the Tor network being the sole large scale system in place. This panel is sponsored by the Panoramix project, which aims to build an anonymous communications infrastructure for applications such as messaging, voting, and survey collection, that offers better privacy protection than Tor. The panel will discuss the goals, challenges, and tradeoffs involved in deploying anonymous communications infrastructures, bringing together technical, legal, policy and civil society perspectives.

- What are the available anonymous communication infrastructures, why do we need them, what do they provide?
- What are the legal, technical and societal challenges to broader deployment of these infrastructures?
- What is the future of anonymous communication networks?

#### 17:15 - CYBER OFFENCE VS PRIVACY DEFENCE

**Academic • Policy • Business •**

**Organised by** Centre for Cyber Law and Policy, University of Haifa

**Chair** Lina Jasmontaite, VUB (BE)

**Moderator** Tal Zarsky, University of Haifa (IL)

**Speakers** Radim Polčák, Masaryk University (CZ), Sofia Casimiro, Academia Militar (PT), Sven Herpig, Stiftung Neue Verantwortung (DE), Bryan Cunningham, UC



Irvine (US)

The cyber realm will be tomorrow's central battle ground. Thus, the importance of cyber-weapons is evident. While governments (and at times non-governmental entities and even private parties) amass their cyber-arsenal, such efforts at times directly conflict with privacy and data security interests. For instance, governments might strive to weaken security systems and conceal vulnerabilities discovered, so they can abuse them when needed. Yet doing so might generate overall privacy and security risks to citizens. Thus, proper standards for vulnerabilities management are urgently needed.

Concerns traditionally existed also with regards to conventional weapons. However, cyber-weapons are fundamentally different, because they affect fundamental rights in peacetime also. Their cross-border nature also brings up new questions regarding re-

lations between privacy and information sovereignty of states. The panel will address such points of conflict, while seeking the proper balance. It will also note the interests involved and the institutions these elements pertain to.

- What would responsible vulnerability management (which accounts for both privacy and data security risks) entail?
- To what extent are privacy and personal data-protective measures limiting defense forces as to procurement of highly destructive cyber-defense measures in peacetime by private parties?
- Which law territorially applies to privacy and data protection in case of cross-border cyber operations?

**18.30 - EPIC CHAMPION OF FREEDOM AWARD** followed by Cocktail sponsored by EPIC in Le Village

## CPDP2018 PANELS AT AREA 42 GRAND

### 8:45 - SIX PROVOCATIONS FOR DATA PROTECTION: FROM PROTECTING CONSUMPTION TO PROMOTING CITIZENSHIP

**Academic •• Policy ••• Business •**

**Organised by** DATAJUSTICE and DATACTIVE

**Chair** Linnet Taylor, Tilburg University (NL)

**Moderator** Stefania Milan, University of Amsterdam (NL)

**Speakers** Anita Say Chan, University of Illinois (US), Arne Hintz, Cardiff Data Justice Lab (UK), Becky Kazansky, University of Amsterdam (NL), Valérie Peugeot,

CNIL/Orange Labs (FR)

Although fundamental rights form the basis for data protection, private-sector lobbying and the objective of facilitating the free flow of data capital both play an important role in the way regulation is formed. Is the central objective of data protection protecting freedom, autonomy and privacy or is it preserving and promoting the EU's position in the global data market? In this session we will challenge participants to return to first principles and ask what kind of data regulation framework would emerge if, for instance, no compromise were possible on freedom,

autonomy and informational privacy; if regulation had to operate on the global scale of the data market, or if it were imperative to prevent future threats to rights stemming from today's practices. Inspired by Boyd and Crawford's 2011 challenge (Six Provocations for Big Data), the session will consist of a roundtable discussion where each participant will present a provocation with regard to data protection, continuing to a group discussion with Q&A.

- What is the balance currently being struck between protecting fundamental rights and promoting the digital single market, and will the GDPR change it?
- Can EU data protection regulation address the global data market?
- What actors and power dynamics could situate rights as the practical focus of regulation?

**10:00 - Coffee break in Lounge Area 42**

### 10:30 - GLOBAL EQUIVALENCE OF DATA PROTECTION REGIMES: HOW TO CREATE BRIDGES BETWEEN DIFFERENT INTERNATIONAL APPROACHES?

**Policy ••• Business •••**

**Organised by** BSA | The Software Alliance

**Chair** Peter Kimpian, Council of Europe (INT)

**Moderator** Michael McEvoy, Office of the Information and Privacy Commissioner of British Columbia (CA)

**Speakers** Thomas Boué, BSA (BE), Adam Schlosser, World Economic Forum (INT), Monika Kuschewsky, Squire Patton Boggs (BE), Vidhya Sampath, Tata Consulting Services (NL)

In many major markets around the world, new data protection laws are set to have a substantial impact on privacy, commerce, cybersecurity, and the development of emerging technologies. Last year, Japan implemented its new privacy law, while India put together an Expert Committee to propose a new data protection system. In 2018, the General Data Protection Regulation comes into force, while additional privacy protections for electronic communications are being negotiated in the EU. No two privacy laws in these major markets are identical. While laws can only apply within a jurisdiction, the data-based economy operates globally. This is a major issue for businesses which seek to transfer data between jurisdictions. This panel will focus on the following questions from a business perspective.

- How will companies, privacy practitioners, and consumers navigate the changing and disparate privacy systems?
- How can governments best work together to create a consistent approach that will provide predictability and stability?
- In how far are different data protection regimes compatible?

### 11:45 - BLOCKCHAIN IN INTELLECTUAL PROPERTY AND DATA PROTECTION: PROMISES AND CHALLENGES

**Academic ••• Policy •• Business •**

**Organised by** International Laboratory for IT and IP Law, Higher School of Economics

**Chair** Leyla Keser, Istanbul Bilgi University (TR)

**Moderator** Ruslan Nurullaev, Higher School of Economics (RU)

**Speakers** Balazs Bodo, University of Amsterdam (NL), Primavera De Filippi, CNRS (FR), Susana Nascimento, JRC

(EU), Guido Noto La Diega, Northumbria University (UK), Alexander Savelyev, Higher School of Economics (RU)

The panel deals with the implications of Blockchain in Intellectual Property Law. In particular it will address the issue of Blockchain-based copyright ownership databases and the conflict between immutability of records v. copyright law. At the same time, it will deal with how to preserve trust in "Smart contracts" as a new way of commercialization of IP.

- How to preserve trust in "Smart contracts" as a new way of commercialisation of Intellectual Property?
- Are Blockchain-based copyright ownership databases an opportunity or a problem for Intellectual Property Law?
- How can Blockchain be an effective solution in data protection law?

**13:00 - Lunch in Lounge Area 42**

#### **14:15 - DATA PROCESSING BENEFICIAL TO INDIVIDUALS: THE USE OF LEGITIMATE INTEREST**

**Academic • Policy • Business •••**

**Organised by** Nymity

**Chair** Raphaël Gellert, Tilburg University (NL)

**Moderator** Aurélie Pols, Mind Your Privacy (ES)

**Speakers** Paul Breitbarth, Nymity (NL), Dominique Hagenauw, Considerati (NL), Leonardo Cervera Navas, EDPS (EU), Gabriela Zafir Fortuna, Future of Privacy Forum (US)

In today's age of the Internet of Things, Artificial Intelligence (AI), cloud computing, mobile devices, advanced analytics and

profiling, it is becoming ever more difficult to obtain valid consent to process an individual's personal data. More organisations are therefore looking to use the legitimate interest ground to process personal data, while at the same time struggling with its correct application. The balancing test needs to be completed, a good overview of potential benefits to individuals when processing their personal data needs to be produced and an ethical assessment needs to be maintained. All this to ensure that the risks of the data processing for the individual are minimised. This panel will discuss various approaches to the use of legitimate interest and the pros and cons of leveraging the benefits to individuals to process personal data.

- What needs to be done to use legitimate interest as a ground for processing personal data under GDPR?
- How do you balance benefits to individuals against risks to their rights and freedoms?
- How does the balancing test contribute to ethical data processing?

**15:30 - Coffee break in Lounge Area 42**

#### **16:00 - DATA PROTECTION AND INNOVATION ACCELERATION**

**Academic •• Policy •• Business ••**

**Organised by** DataPitch

**Chair** Malte Beyer-Katzenberger, DG CNECT (EU)

**Moderator** Sophie Stalla-Bourdillon, University of Southampton (UK)

**Speakers** Paul Francis, Max Planck Institute for Software Systems (DE), Evelyne Gebhardt, MEP (EU), Bashara Hinnawi, Beta-i (PT), Alison Knight, University of Southampton (UK), Gary Lafever, Anonos (US), Gwendal le Grand, CNIL (FR)

COMPUTERS, PRIVACY & DATA PROTECTION

The EU digital single market promotes open data innovation - bringing together corporate and public sector organisations wanting to discover the untapped opportunity in their data, on the one hand, together with the skills of startups and SMEs exploring such data on the other. The biggest challenge in achieving this vision is how to make open innovation sustainable in the long run. Yet, EU data protection law is often depicted as a barrier to unleashing the full potential of open innovation in that it over-constrains internal and external data analytics practices. The aim of this panel is to discuss and assess the results of recent innovation acceleration initiatives and the data protection challenges that arise in these contexts as contributions to building the European data economy.

- How can we overcome legal and technical obstacles to unleash the full potential of closed datasets through data sharing in order to promote open innovation?
- How does data protection and privacy laws impact upon closed data sharing practices?
- To what extent are anonymisation and pseudonymisation solutions crucial in a closed environment and for open innovation acceleration?

#### **17:15 - THE PERFECT MATCH? A CLOSE LOOK AT THE RELATIONSHIP BETWEEN CONSUMER LAW AND DATA PROTECTION LAW**

**Academic ••• Policy •• Business •**

**Organised by** Universiteit van Amsterdam (IVIR)

**Chair** Ursula Pachi, BEUC (BE)

**Moderator** Natali Helberger, University of Amsterdam (NL)

**Speakers** Julie Brill, Microsoft (US), Joseph Turow, Annenberg School of

THE INTERNET OF BODIES

Communication (US), Evelyne Gebhardt, European Parliament (EU), Justine Masera, UFC Que Choisir (FR)

In the Internet of Bodies, consumers will be surrounded by data-driven products and services. The trading and consumption of these data-driven services fall under two separate sets of rules: consumer law and data protection law. There is little knowledge and experience about how these rules interact and can usefully complement each other. The objective of this panel is to explore how data protection and consumer law could complement each other to better protect consumers in these fast-developing data-driven markets. Special focus will be on the ongoing legislative developments at EU level, but also how to harvest the expertise and experience from the US and EU about how to approach the interactions between consumer and data protection law.

- What can the US approach towards privacy protection through consumer law contribute to the European debate?
- Free services and paying with your data and the Draft digital Content Directive
- Relationship consumer law/data protection law
- EU-US – Transatlantic Dialogue

**18:30 - EPIC CHAMPION OF FREEDOM  
AWARD followed by Cocktail  
sponsored by EPIC in Le Village**

## CPDP2018 PANELS AT AREA 42 PETIT

### 8.30 - WELCOME AND INTRODUCTION IN GRANDE HALLE

### 8:45 - ROBOTS IN THE CLASSROOM – NEW LEARNING VISIONS IN THE TECHNOLOGICAL ERA

**Academic • Policy • Business •**

**Organised by** MaTHiSiS project

**Chair** Oonagh Shannon-Roche, ELF (BE)

**Moderator** István Böröcz, VUB (BE)

**Speakers** Janice Richardson, INSIGHT S.A. (LU), Eszter Salamon, EPA (BE), Régis Chatterlier, CNIL (FR), Andrea Cira, FMD, ARCI (IT)

This panel takes inspiration from the activities and findings of an ongoing Horizon2020 research project which seeks to develop an integrated platform for the education of both mainstream learners and learners with special needs. New techniques such as learning analytics, adaptive learning, automatic feedback, affective computing and game-based learning allow for the personalisation of the learning experience. However, it seems that it will still “take a village to grow a child”, even in the digital age. In addition to teachers and schools, parents have a duty to take care of their children online, but to what extent? Teachers and schools routinely process personal data to achieve didactic purposes, or to conduct research. In addition to practical regulatory issues, the debate over children and technology raises a number of other legal, societal and ethical questions. These will be discussed by a panel composed of a clinical and community psychologist, a social scientist, a teacher and legal experts.

- How will article 8 of the GDPR empower or inhibit the participation of children in

the information society?

- How does continuous interaction with technologies affect learning and the capacity to establish relationships with others and the world?
- As surveillance scholar Gary T. Marx asks in Windows into the Soul: Will the habit of technology surveillance at school somnolently create dependency, so that learners of today will be the docile subjects of surveillance tomorrow?

### 10:00 - Coffee break in Lounge Area 42

### 10:30 - PERSONAL DATA: STILL A RELEVANT TRIGGER FOR PROTECTION IN A DATA-DRIVEN SOCIETY?

**Academic • Policy • Business •**

**Organised by** ERC INFO-LEG Project

**Chair** Maryant Fernandez Perez, EDRI (BE)

**Moderator** Nadezhda Purtova, Tilburg University (NL)

**Speakers** Peter Hustinx, former EDPS (NL), Maurits Kaptein, Tilburg University (NL), David Stevens, Nielsen (BE), Frederik Zuiderveen Borgesius, VUB (BE)

The goal of this panel is to explore the relevance of the notion of personal data as a trigger for the application of data protection law now and in the near future. Given the broad understanding of the notion adopted 10 years ago by the Article 29 Working Party, and in today's context characterized by machine learning and big data analytics, the argument is becoming increasingly plausible that any piece of information can legally become personal data. During the panel, we will retrace the origins and rationale of the notion, and further explore its meaning both

from a legal and computer science/machine learning perspective.

- Given the current state of data analytics is there any data that does not relate to people in a legal sense?
- Can e-privacy serve as a blueprint for non-personal data centric legal protection?
- Could we envisage a data protection framework not based on the notion of personal data?

### 11:45 - CIVIL ENGAGEMENT: A BLUE- PRINT TO BUILD CLOSER COOP- ERATION BETWEEN BUSINESS AND CIVIL SOCIETY

**Academic • Policy • Business •**

**Organised by** Privacy Surgeon

**Chair** Barry Guihen, VUB (BE)

**Moderator** Nicolas Martin, Fraunhofer ISI (DE)

**Speakers** Simon Davies, Privacy Surgeon (UK), Hielke Hijmans, CIPL (NL), Annie Machon, Security expert and whistleblower (BE), Michael Collyer, University of Amsterdam (NL);

In 2017, a coalition of corporations and NGO's joined to support an initiative to create a more cooperative and constructive relationship between activists, government and the private sector. Since that time, veteran privacy activist Simon Davies has been consulting to discover ways to make this happen. The results are surprising. Almost none of the small companies surveyed had any contact whatsoever with civil society. Venture Capital companies and investors almost never engage. Medium size companies in the information realm are increasingly seeing the potential of a stronger connection, but this is currently little more than an intellectual exercise. Among the large companies surveyed, almost none

had an internal engagement strategy that had any measurable impact on operations. However, where engagement has occurred it has created powerful benefits. In this session, Davies and other panelists will host an interactive discussion of how – or whether – such a closer relationship is possible. The session will launch the interim report of the project.

- Should civil society even consider the benefits of engagement with business and government? Is such a relationship unsustainable in an activist environment?
- What are the limits to engagement by companies? Is such a potential relationship too risky for corporate stakeholders?
- What – if anything – do we want to achieve by building closer relations?

### 13:00 - Lunch in Lounge Area 42

### 14:15 - JUNIOR ACADEMIC SESSION 1: THE INTERNET OF BODIES

**Academic •**

**Organised by** CPDP

In the first Academic Session of CPDP 2018, the authors will explore the link between physical bodies and digital information. Sax, Bol, and Helberger will discuss mHealth apps, and the delicate balance between profit and autonomy. Zouave and Schroers will then delve into the processing of biometric data in the context of criminal justice. Vierbergen will conclude the session exploring the effect of individual data doubles on individual bodies. The session will be chaired by Laurent Beslay (JRC).

- Marijn Sax (University of Amsterdam), Nadine Bol (University of Amsterdam) and Natali Helberger (University of Amsterdam). Health as a Means Towards Profitable Ends? mHealth Apps and the Precarious Balance Between Commerce and User Autonomy

# Thursday 25 January 2018

## CPDP2018 PANELS AT GRANDE HALLE

- Erik Zouave (Swedish Defence Research Agency) and Jessica Schroers (KU Leuven). You've been Measured, You've been Weighed & You've been Found Suspicious: Biometrics & Data Protection in Criminal Justice Processing
- Mick Vierbergen (University of Amsterdam). Nerves at the Border: How Dividual Data Doubles Affect Individual Bodies

### 15:30 - Coffee break in Lounge Area 42

#### 15.30 - DATA MINIMIZATION BY DESIGN

**Organised by** CNIL-Inria 2017 Privacy

Award

**Chair** Daniel Le Metayer (INRIA)

Presentation on privacy engineering and data minimization by design by the winners of the CNIL-Inria 2017 Privacy Award

#### 16:00 - ACADEMIC SESSION 2: CODE AND THE LAW

**Academic .....**

**Organised by** CPDP

The second Academic Session is about code, the law, and the impact of their interaction on society at scale. Liebert will present the results of an empirical, web-scale analysis of the "notice and choice" paradigm. Emanuilov and others will deal with how to embed privacy and data protection into the very fabric of software by acting on its design. Noto La Diega concludes the session, reporting on the outcome of a qualitative study on "platforms for men who have sex with men", privacy, and discrimination. The session will be chaired by Alessandro Mantelero, (NEXA Center for Internet and Society)

- Timothy Libert (University of Oxford). On the Impossibility of Accepting the Unknown: A Web-Scale Analysis of the Fail-

ure of Notice and Choice

- Ivo Emanuilov (KU Leuven), Kim Wuyts (KU Leuven), Dimitri Van Landuyt (KU Leuven), Natalie Bertels (KU Leuven), Fanny Coudert (KU Leuven), Peggy Valcke (KU Leuven) and Wouter Joosen (KU Leuven). Navigating law and software engineering towards privacy by design: stepping stones for bridging the gap
- Guido Noto La Diega (Northumbria University). "Some body that I used to own". An empirical qualitative research on privacy, discrimination, and platforms for men who have sex with men

#### 17:15 - JUNIOR ACADEMIC SESSION 3: THE INTERNET OF US

**Academic .....**

**Organised by** CPDP

Technology is inherently political, and has regulatory capacity. In the third Academic Session of CPDP2018, the authors will explore the societal implications of three particular facets of technological innovation. Lanzing will discuss self-tracking, between nudging and autonomy. Jasserand will deal with face recognition in light of the GDPR. Ishmaev will close the session, by reframing the concept of trust in the Internet of Things. The session will be chaired by Ronald Leenes (TILT).

- Marjolein Lanzing (TU Eindhoven). Coaching or Coaxing? Self-tracking, Hypernudging and Decisional Privacy
- Catherine Jasserand (University of Groningen). MegaFace under the magnifying glass of the General Data Protection Regulation
- Georgy Ishmaev (TU Delft). Rethinking trust in the Internet of Things

#### 18.30 - EPIC CHAMPION OF FREEDOM AWARD followed by Cocktail sponsored by EPIC in Le Village

COMPUTERS, PRIVACY & DATA PROTECTION

#### 8:45 - CAN CITIZENSHIP OF THE TARGET EVER BE A JUSTIFIED BASIS FOR DIFFERENT SURVEILLANCE RULES?

**Academic .. Policy ... Business ..**

**Organised by** Georgia Institute of Technology

**Chair** Wendy Grossman, Independent Journalist (US)

**Moderator** Amie Stepanovich, Access Now (US)

**Speakers** Joseph Cannataci, UN Special Rapporteur on the Right to Privacy (INT), Mario Oetheimer, Fundamental Rights Agency (EU), Peter Swire, Georgia Institute of Technology (US), Thorsten Wetzel, Stiftung NV (DE)

This panel will examine the topic of whether the nationality of an individual under surveillance (the "target") is and should be relevant to the legal standards for surveillance. Legislation in effect today, in countries including the United States and Germany, applies stricter protections for national security surveillance of a nation's own citizens than for foreigners. To date, there has been no systematic discussion of whether and on what basis those stricter standards might be justified. Some writers have asserted a "universalist" position, that national security surveillance must apply identically to both citizens and non-citizens. This panel will provide a description of current law and practice. It will then discuss and debate whether, and in what circumstances if any, it may be justified to apply different surveillance standards based on whether the individuals under surveillance have citizen-

THE INTERNET OF BODIES

ship or other significant connections to the country undertaking the surveillance.

- According to the rules for access to data under the Mutual Legal Assistance process, a nation may have greater access to information held abroad about its own citizens. Is it acceptable and adequate?
- Discussion of international human rights reasons for equivalent treatment of individual targets, irrespective of the target's nationality.
- Can different rules apply to surveillance undertaken in situations involving war and foreign affairs?

### 10:00 - Coffee break in Le Village

#### 10:30 - HOW YOUR FAVOURITE APPS HAVE AND WILL CHANGE WITH GDPR AND EPRIVACY?

**Academic .. Policy .. Business ...**

**Organised by** OneTrust

**Chair** Bojana Bellamy, CIPL (US)

**Moderator** Kabir Barday, OneTrust (UK)

**Speakers** Prokopis Drogkaris, ENISA (EU), Zoe Kardasiadou, EDPS (EU) tbc, Geert Somers, time.lex (BE), Speaker tbc

You may not realise just how much personal data your favourite apps collect. That will soon change under the General Data Protection Regulation (GDPR) and proposed ePrivacy Regulation. Starting May 25, 2018, almost every app, whether it's desktop, mobile, enterprise, or consumer, will face new legal hurdles, making behind-the-scenes, unnecessary collection of your personal data ill-advised. But how will these new protections



affect user experience? Will personal privacy come at the expense of functionality?

- How will the stricter definition of consent affect popular social media applications?
- How do you foresee application developers applying privacy by design principles and data portability to existing applications?
- How will advertising models for many applications change as a result of the GDPR and proposed ePrivacy regulation?

#### 11:45 - SMARTPHONES AND WEARABLES AS CONNECTED BIOINFORMATICS HUBS – SECURITY AND PRIVACY CONCERNS

**Academic • Policy • Business •**

**Organised by** Huawei

**Chair** John Howie, Huawei Technologies (US)

**Moderator** Agnieszka Wawrzyk, European Commission (EU)

**Speakers** Joan Antokol, Park Legal LLC (US), Hadi Asghari, TU Delft (NL), Maarten Bodlaender, Philips (NL), Speaker tbc

The General Data Protection Regulation, as did the Data Protection Directive, defines health-related data as a special category of personal data. Increasingly, sensors are being built into smartphones and wearables such as watches and general fitness trackers. These devices are becoming integrated with each other, and cloud based services over cellular networks. This pace of innovation will only accelerate with new devices and 5G technologies. The panel will discuss at which point the benefits of connected healthcare devices monitoring for hypertension, heart attacks, strokes, or slips and falls amongst vulnerable members of society are outweighed by privacy and security concerns, as well as connected pacemakers, insulin pumps, and others.

- Will insurance companies be permitted to

access data and use it to drive premiums or deny healthcare to individuals with unhealthy lifestyles?

- Will device manufacturers and telecommunications companies monetize observed data through advertising?
- If devices are bidirectional, can they be hacked and what will the outcome be – will people die?

#### 13:00 - Lunch in Le Village

#### 14:15 - CONVENTION 108: CONVERGENCE AND EXPANSION

**Academic • Policy • Business •**

**Organised by** Council of Europe

**Chair** Malavika Jayaram, Digital Asia Hub (IN)

**Moderator** Bruno Gencarelli, DG Just (EU)

**Speakers** Sophie Kwasny, Council of Europe (INT), Patricia Poku, DP Commission (GH), Fernando Sosa, INAI (MX), Gonzalo Sosa, URCPDP (UR)

With increasingly ubiquitous data flows, the best –and only– way to ensure that each person is effectively protected with regard to the processing of personal data, is to provide at global level, a common acceptance of fundamental principles in the field of data protection. It is precisely to this end that Convention 108 was designed. It is unique in its opening on the world: no other instrument can provide such a global forum of cooperation and harmonisation. Nearly 70 countries are currently part of the work carried out in the framework of the Convention. Panellists will focus on the benefits of accession to the Convention and its articulation with the framework of the European Union.

- What are the further realistic prospects of globalisation (already 51 parties)?
- Why acceding? Economic advantages? Human rights flagship?

- Convention 108 and the EU Data Protection framework: how and why are they converging?

#### 15:30 - Coffee break in Le Village

#### 16:00 - THE ROLE OF ETHICAL ANALYSIS IN PRIVACY AND DATA PROTECTION ASSESSMENTS

**Academic • Policy • Business •**

**Organised by** TrustArc

**Chair** Chris Babel, TrustArc (US)

**Moderator** Dennis Hirsch, Ohio State University Moritz College of Law (US)

**Speakers** Gemma Clavell, Eticas (ES), Gry Hasselbalch, DataEthics (DK), Evert-Ben van Veen, Medlawconsult (NL), Hilary Wandall, TrustArc (US)

The role of risk in conducting privacy and data protection assessments has been an area of recent regulatory focus, however the broader role of ethical considerations remains largely undefined. This panel will consider the role of ethical analysis in undertaking privacy and data protection assessments (e.g., DPIAs, PIAs and LIAs) contemplated by laws such as the EU GDPR. Using cross-disciplinary and historical lenses, the panelists will explore the way in which ethical principles, such as those set forth by Beauchamp and Childress, have been evaluated in other forms of ethical review and ethical impact assessment, and how they relate to and may be applied to privacy and data protection assessments.

- How do ethical considerations factor into DPIAs, PIAs and LIAs?
- What is similar and/or different across each of these assessment types? Are certain ethical principles more important than others?
- What lessons from other applications of ethical assessments and reviews are useful to the design and implementation of

privacy and data protection assessments?

#### 17:15 - VALUES AND SHIFTS IN THE DIGITAL AGE

**Academic • Policy • Business •**

**Organised by** European Data Protection Supervisor (EDPS)

**Chair** Giovanni Buttarelli, EDPS (EU)

**Moderator** Jim Dratwa, European Commission (EU)

**Speakers** Peter Burgess, Ecole Normale Supérieure Paris (FR), Antoinette Rouvroy, University of Namur (BE), Jeroen van den Hoven, TU Delft (NL), Aurélie Pols, Data Governance & Privacy Engineer (ES)

Two years ago the European Data Protection Supervisor (EDPS) established an Ethics Advisory Group (EAC) to explore the relationships between human rights, technology, markets and business models in the 21st century. Members of the Group will present the state of play of their report Toward a Digital Ethics, mapping and analysing current and future paradigm shifts of society from analogue to digital. In light of this shift, the report aims to refresh our understanding of the fundamental values essential to maintaining the well-being of society as a whole and those values that are taken for granted in our data-driven lives, particularly those most at risk. The purpose of the report is not to put forward definitive answers, but to identify the critical questions that need to be addressed including:

- What is the impact of the turn to a “scored society”?
- How is responsibility distributed in the digital eco-system?
- How is data being commoditized in current data markets?

#### 18.30 - Cocktail followed by EDPS, FPF and Qwant Panel on Privacy by Design

## CPDP2018 PANELS AT PETITE HALLE

### 8:45 - FINDING A WAY FORWARD FOR CROSS-BORDER DATA REQUESTS

**Academic • Policy • Business •**

**Organised by** Institute for Policy in Medicine and Law at Washington University

**Chair** Vanessa Franssen, KU Leuven (BE)

**Moderator** Neil Richards, Washington University School of Law (US)

**Speakers** Jennifer Daskal, American University (US), John Frank, Microsoft (BE), Ralf Sauer, DG Just (EU), Eduardo Ustaran, Hogan Lovells (UK)

Lawful access regimes for the Cloud require a careful balancing of interests of government, technology companies, and the individuals and organizations using the cloud. The problem of what standards should govern lawful access becomes significantly more complex in international settings. Relevant questions have traditionally been resolved at the national level and through a complicated web of MLATs. But this regime is strained by the volume of requests and questions of adequacy of foreign standards. Unsurprisingly, these issues have prompted high-profile litigation involving Microsoft, Facebook, Yahoo, and others in cases involving extraterritorial requests. The international communities of technologists, privacy lawyers, and law government officials at odds about many fundamental questions. Yet even when we can identify answers, cultural and political issues can easily get in the way. This panel attempts to bridge some of those barriers with a discussion by a diverse group of experts from Europe and the U.S.

- When should the U.S. government be able to obtain users' private communications

from companies located in the U.S. when the data (and possibly the customers) are located in Europe?

- What should happen when European law enforcers seek data about Americans from the European subsidiaries of U.S.-based technology companies?
- How can commitments to consumer and citizen privacy be reconciled with the need for at least some government access?

### 10:00 - Coffee break in Le Village

### 10:30 - SHATTERING ONE-WAY MIRRORS: THE RIGHT OF ACCESS IN PRACTICE

**Academic • Policy • Business •**

**Organised by** Centre for IT & IP Law (CIT-IP) KU Leuven

**Chair** Jef Ausloos, KU Leuven (BE)

**Moderator** Anna Buchta, EDPS (EU)

**Speakers** Paul-Olivier Dehay, Personal-data.io (CH), Edina Harbinja, Hertfordshire University (UK), Hal Hodson, The Economist (UK), Alison Howard, Microsoft (US)

This panel aims to shed light on the effectiveness of the data subject right to access in the context of information society services. The panel will present the findings of recently conducted legal-empirical analysis of sixty online service providers and their compliance with the rights of access and erasure. With this as a starting point, the panel will invite different stakeholders to react and contextualise the findings as well as suggest practical next steps. The panel will clarify the importance of this data subject right via the illustrative examples of investigative data journalism and post-mortem data protection. Building

on this, industry, civil society and academic perspectives will give depth to the debate.

- Why is it important, from a practical perspective, to ensure an effective right of access?
- What are the main thresholds/barriers for rendering effective the rights of access/erasure in practice?
- How to ensure higher compliance levels with data subject rights? What is the role of academia?

### 11:45 - GENDERED DATA BODIES

**Academic • Policy • Business •**

**Organised by** CPDP

**Chair** Gloria González Fuster, VUB (BE)

**Moderator** Rocco Bellanova, University of Amsterdam (NL)

**Speakers** Ana Brandusescu, World Wide Web Foundation (UK), Seeta Peña Gangadharan, LSE (UK), Grégoire Marino, Clue (DE), Valentina Hvale Pellizzer, Association for Progressive Communications (ZA)

Online data collection and processing are often portrayed as gender-less practices. Gender, however, can play a determinant role in the ways in which our bodies are apprehended, mediated and modulated through data. Also, besides -and beyond- gender, other dimensions may need to be (better) integrated in the ways in which we understand and frame contemporary data realities. This panel aims to foster these discussions by considering data bodies from a gendered and intersectional perspective, discussing the practical functioning and possibilities of menstrual tracker apps, exploring the connections between online information and sexual education and expression, and inquiring about the global challenges in this area. It will notably ask:

- What is special about girls' and women's

experiences of data sharing and processing, and what can we learn about them through increasingly popular menstrual trackers?

- What do we know about the relations between the Internet, sexual expression, sexualities and sexual health practices?
- How to think globally about feminist data politics, with and beyond gender?

### 13:00 - Lunch in Le Village

### 14:15 - REGULATING FOR RESULTS

**Academic • Policy • Business •**

**Organised by** Centre for Information Policy Leadership (CIPL)

**Chair** Yukiko Lorenzo, MasterCard (BE)

**Moderator** Hielke Hijmans, CIPL (NL)

**Speakers** Wilbert Tomesen, Autoriteit Persoonsgegevens (NL), Elise Muir, KU Leuven (BE), Marie-Charlotte Roques Bonnet, Microsoft (FR), Richard Thomas, CIPL (UK), Wojciech Wiewirowski, EDPS (EU)

The aim of this panel is to stimulate discussion about how DPAs can maximise their effectiveness. When functions are numerous, expectations are high and resources are limited the paper asks whether - and how - conscious efforts should be made for the regulation of data protection to become "Smart". This involves making difficult, but essential, choices about strategies and priorities. DPAs simply cannot do everything.

Smart data protection means DPAs - independently and co-operatively - maximising their effectiveness by adopting modern and strategic approaches on regulation. In particular, this involves responsively engaging with, and supporting, those organisations - private and public sector - which are ethically seeking to "get it right". But it also means dealing firmly with those who are not trying.

- When the responsibilities of most DPAs are so numerous, what are the best ways to achieve overall effectiveness?
- Which ways should be explored for increasing DPA budgets to more realistic levels?
- What can be learned from approaches which have been adopted around the world in many other spheres of regulation?

15:30 - Coffee break in Le Village

#### 16:00 - PRIVACY, ADVERTISING, AND TRUST: CAN WE HAVE IT ALL?

**Academic • Policy • Business •**

**Organised by** Mozilla

**Chair** Raegan MacDonald, Mozilla (BE)

**Moderator** Jennifer Baker, EU Tech Policy Reporter (BE)

**Speakers** Catherine Armitage, World Federation of Advertisers (BE), Anna Ciesielska, DG CNECT (EU), Laura Dornheim, Adblock Plus (DE), Mathilde Fiquet, FEDMA (BE), Estelle Massé, Access Now (BE)

Like it or not, there's no denying that advertising is the dominant business model of the web today. This business model has allowed a range of quality services and websites to operate without requiring direct payment by end users. However, this approach has contributed to a severe erosion of trust in the online ecosystem - evidenced both anecdotally, through statements like "if you're not paying, then you're the product", and practically, through a sharp increase in content blockers. Ad fraud, pervasive tracking, diminishing returns, all further separate the publisher from the user. While advertising itself may not be the problem, the current status quo is unsustainable. So how can we get that trust back? What kind of reforms would make progress towards meaningful changes that would

help achieve harmony between user trust and economic business models? This panel will unpack these questions with a view to forging a first step towards a long term, sustainable vision for the future of the web.

- What kind of reforms would make progress towards meaningful changes that would help achieve harmony between user trust and economic business models?
- How can the ad industry benefit from privacy compliance?
- Are there alternative business models that could rival and/or co-exist with advertising?

#### 17:15 - HOW CAN INDUSTRY STANDARDS SUPPORT GDPR COMPLIANCE?

**Academic • Policy • Business •**

**Organised by** Microsoft

**Chair** Prokopios Drogkaris, ENISA (EU)

**Moderator** Alex Li, Microsoft (US)

**Speakers** Babak Jahromi, Microsoft (US), Clara Neppel, IEEE (US), Jan Schallaböck ISO (INT), Manuela Siano, Garante per la protezione dei dati personali (IT)

As the 25<sup>th</sup> of May approaches, controllers and processors seek to identify tools to help them comply with the obligations imposed by the GDPR. Industry standards are important to the development of the Internet and to interoperability among mobile, other interconnected devices and the digital services they communicate with. The discussion will shed light in recent developments in the activity of standard-setting organisations and will offer the perspective of the data protection authorities.

- What type of standards are relevant for various GDPR obligations (data portability, data protection by design, etc.)?

COMPUTERS, PRIVACY & DATA PROTECTION

- Are standards and certification a 'mandatory' element of GDPR accountability? Or are they complementary?
- Will data protection authorities treat non-conformity to standards and certification as aggravating factor to non-compliance?

## CPDP2018 PANELS AT LA CAVE

#### 8:45 - DATA PROTECTION HARMS IN PRIVATE LAW: LEVELLING THE PLAYING FIELD FOR DATA SUBJECTS?

**Academic • Policy • Business •**

**Organised by** Radboud University, Nijmegen

**Chair** Stefano Leucci, Polytechnic University of Turin (IT)

**Moderator** Mireille Hildebrandt, VUB (BE)

**Speakers** Valerie Lyons, BH Consulting (IE), Tim Walree, Radboud University, Nijmegen (NL), Pieter Wolters, Radboud University, Nijmegen (NL), Speaker tbc

This panel discussion will focus on the issues around the notion of private law liability (injunctions and/or compensation) with regard to data protection violations. Next to enforcement by Data Protection Supervisors, private law enforcement may become an essential mechanism for safeguarding data protection. However, rarely do data subjects initiate a procedure against a data controller or processor for breaching rules of data protection law. Litigating can take long, procedural costs can be high and gathering of evidence can be problematic. Harmed data subjects may therefore be reluctant to bring a case before court. If data subjects never-

theless decide to start a procedure, they will in principle bear the burden of proof that harm is caused, raising the question of what constitutes a data protection harm, as tort law requires a concrete (material or immaterial) harm. Furthermore, a violation of data protection law, and causality between such violation and the harm, must be established. This may be burdensome, given the complexity of data processing operations as well as the continuously increasing amount of organisations that process personal data, even if harm can be proven. In light of these constraints, this panel will discuss tort law's potential contribution to a level playing field between data subjects and data controllers and processors.

- What should constitute a data protection harm?
- How should courts deal with the issue of causality (e.g. reversal of the burden of proof, loss of chance, proportional liability)?
- What solutions does and/or should the GDPR offer to the unequal playing field? Which solutions are offered by national regimes of tort law?

10:00 - Coffee break in Le Village

THE INTERNET OF BODIES

# 11<sup>th</sup> INTERNATIONAL CONFERENCE 24 25 26 JANUARY 2018 BRUSSELS, BELGIUM

# COMPUTERS, PRIVACY & DATA PROTECTION 2018

# THE INTERNET OF BODIES



PLATINUM



PREMIER



EVENT SPONSORS



MORAL SUPPORTERS

MEDIA PARTNERS



EVENT PARTNERS



EVENT PARTNERS



CONFERENCE PARTNERS



CONFERENCE PARTNERS



### 10:30 - COMBINING BUSINESS PROTECTION AND PRIVACY PROTECTION PRACTICES IN BIG DATA MARKET PLACES

**Academic • Policy • Business •**

**Organised by** AUTOMAT Project

**Chair** Antonio Kung, Trialog (FR)

**Moderator** Andriy Ilyuk, Göttingen University (DE)

**Speakers** Xuebing Zhou, Huawei (DE), Natalie Bertels, KU Leuven (BE), Giulia Marcocchia, IMT Paris (FR), Thierry Nagelen, Orange (FR)

Big data market places will allow stakeholders to publish, exchange and combine datasets. But there are two important concerns: from a business viewpoint it will be important to ensure that a dataset does not reveal a trade secret, or that IPR is enforced along the business chain; from a privacy viewpoint one has to ensure that a dataset does not reveal personal data unless consent is provided. In this further case one has to ensure that it is possible to comply with a citizen's request to remove their personal data.

Further to a video introduction provided by Ann Cavoukian (Ryerson Institute), we will invite the panel to reflect on these concerns. Use cases where data is initially collected for business purpose will be considered (e.g. mobile data collected by telecommunication operators, vehicle data collected by automotive manufacturers). Business, technical, contractual and interoperability issues will be discussed.

- Are there business models that would create synergy between personal data ecosystems and business data ecosystems?
- Are there technology approaches that would create synergy between mechanisms for business confidentiality and mechanisms for anonymisation?

- Are there contractual approaches that would create synergy between big data IPR management and citizen privacy rights management?

### 11:45 - DATA-DRIVEN INNOVATION, PRIVACY AND NATIONAL SOVEREIGNTY IN A GLOBAL WORLD

**Academic • Policy • Business •**

**Organised by** Google Chair on Privacy, Society and Innovation, Universidad CEU San Pablo

**Chair** José Luis Piñar, Universidad CEU San Pablo (ES)

**Moderator** Victoria Nash, Oxford Internet Institute (UK)

**Speakers** Michael Camilleri, Inter-American Dialogue (US), Edison Lanza, Organization of American States Special Rapporteur for Freedom of Expression (INT), Ariane Mole, Bird & Bird (FR), Dan Svantesson, Bond University (AU)

The increasing global interdependence and the advances that data-driven innovation, the use of artificial intelligence and the digitization of processes and activities bring dilute the physical frontiers posing a series of challenges from the perspective of the nation-state. Collaborations between states and the forging of alliances between territories that have to respond to some of the issues that arise in this new context where privacy and other fundamental rights and values, like freedom of expression or transparency, must be protected in an interconnected and global world. This issue also arises when a private company must respond to legal requirements of jurisprudence, national laws or international instruments, proposing different models of action and particular approaches in a context of increasing globalization and worldwide businesses.

- What are the limits of a state jurisdiction and what scope does the recognition of digital rights have for citizens?
- What challenges face the main actors of technological innovation in a global world when they must respond to criteria established by different legal cultures?
- In terms of reciprocity, what consequences can we expect when dealing with the extraterritorial application of rules forged under other legal culture and legislative body other than our own?

### 13:00 - Lunch in Le Village

### 14:15 - (DISRUPTIVE/ENABLING) TECHNOLOGIES, ETHICS AND THE GDPR

**Academic • Policy • Business •**

**Organised by** Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg

**Chair** Mark Cole, Saarbrücken Institute of European Media Law (DE)

**Moderator** Andra Giurgiu, University of Luxembourg (LU)

**Speakers** Maja Brkan, Maastricht University (NL), Mathilde Stenersen, Commission Nationale pour la Protection des Données (LU), Charles Raab, University of Edinburgh (UK), Erik Valgaeren, Stibbe (BE)

This panel will discuss the role of technology in the context set up by the GDPR as having both an enabling and a disruptive potential. Technologies, like AI, which can fulfill both of these functions, will be debated. At the same time, a closer look at specific provisions of the GDPR, such as the Article 22 provision on automated decision-making, will examine potential limits set by the Regulation in the use of these technologies. Ethics, as an underlying value to be considered in the way information technologies

are designed and deployed, will be the lens through which these issues have to be examined, in view of ensuring general respect for fundamental rights. The discussion will also include issues of whether and how IT can actually be used in the practical enforcement of the GDPR.

- Is technology enabling or rather disrupting the application of the GDPR?
- How can we use technology as an enabler and what are the limits we choose to set for technologies having the potential to be disruptive?
- What are the limits for the practice and how to overcome them?

### 15:30 - Coffee break in Le Village

### 16:00 - PRIVACY AND DATA PROTECTION ISSUES RELATED TO THE USE OF MULTIMODAL BIOMETRICS 'ON-THE-MOVE' AT BORDER-CROSSINGS

**Academic • Policy • Business •**

**Organised by** University of Namur in behalf of the PROTECT Project

**Chair** Diana Dimitrova, FIZ Karlsruhe (DE)

**Moderator** Cecile de Terwangne, University of Namur (BE)

**Speakers** Franck Dumortier, University of Namur (BE), Frank Schmalz, VERIDOS (DE), Mikko Simola, Permanent Representation of Finland to the EU (FI), Lara Smit, EDPS (EU)

In order to facilitate the security and fluency of Schengen Area external cross-border movements, projects propose to develop multimodal biometric solutions for contactless identity confirmation of travellers. For the purposes of multimodal biometric ID verification, project partners proposed

to design and develop a biometric corridor, which would incorporate a number of biometric sensors. The initial plan is to include such biometrics as: face recognition, iris recognition, vein pattern recognition, speaker recognition as well as anthropometric recognition. When operational, the beneficiaries of the multimodal biometric system being developed should be persons enjoying the Union right of free movement as well as third country nationals. This session will bring together academic experts in the field of data protection at border-crossings and policy representatives to discuss the privacy implications of contactless multimodal biometrics at the external borders.

- How to improve the border control process with new biometric modalities and increase convenience and speed? Practical aspects.
- Legal constraints deriving from legislation regulating EU travel documents, Schengen IT systems and legislation regulating privacy and data protection?
- Contactless biometrics in the context of the legislative initiatives related to Smart Borders and "interoperability" of large-scale IT databases?

#### 17:15 - \*INFORMATIONALIZATION\* OF BODY SIGNALS AND CRIMINAL INVESTIGATIONS

**Academic ... Policy .. Business ..**

**Organised by** University of Basel

**Chair** Stephanie Pell, West Point's Army Cyber Institute (US)

**Moderator** Sabine Gless, University of Basel (CH)

**Speakers** Jan-Philipp Albrecht, MEP (EU), David Gray, University of Maryland School of Law (US), Dominik Herrmann, University of Bamberg (DE), Miltos Kyriakidis, ETH-Singapore Centre

(Singapore)

Connecting man to machine is a prerequisite for the safe digitalisation of our living environment. Smart driving offers several benefits. Currently, for instance, car manufacturers are installing drowsiness detection systems that monitor a driver's behaviour. Sensors note breathing changes, head and eye movements, body posture, heart rate as well as body temperature and algorithm based systems review the information for patterns that are typical of someone who is sleepy, giving a warning before such tiredness actually poses a risk.

Although advertisements suggest that this man-machine-connection works for the best of the driver only, various issues arise, to start with, concerning the data, which is regularly stored with the car manufacturer, including:

- Who may use the data for their own purposes? And in case of an accident, can the data be used against the driver without violating the privilege against self-incrimination?
- What bodily data do smart cars read and digitalize, and who has access for what purposes?
- Should regulators encourage big data usage of such body data in order to prevent accidents, eventually looking for a man to man connection?
- Should prosecution services be allowed to use such data in a criminal trial against a driver, or possibly in the future, against the passenger of a car?

#### 18.30 - Cocktail followed by EDPS, FFP and Qwant Panel on Privacy by Design in Le Village

## CPDP2018 PANELS AT AREA 42 GRAND

### 8:45 - CAN DEMOCRACY SURVIVE BIG DATA AND MICRO-PROFILING IN ELECTIONS?

**Academic .. Policy .. Business ..**

**Organised by** Centre for Digital Democracy and Transatlantic Consumer Dialogue

**Chair** Paul-Olivier Dehaye, Personaldata.io (CH)

**Moderator** Anna Fielder, Transatlantic Consumer Dialogue (UK)

**Speakers** Jeffrey Chester, Center for Digital Democracy (US), Juhi Kulshrestha, Hans Bredow Institute for Media Research (DE), Michael McEvoy, Office for Information and Privacy Commissioner of British Columbia (CA), Irina Vasiliu, DG Just (EU), Speaker tbc

Today's political candidates and issue campaigns are fully integrated into the growing Big Data marketing infrastructure, with more and more companies in this sphere accelerating the pace of research and innovation and promising to transform how political campaigns and elections are conducted. Data management platforms, marketing clouds, and other new data services enable information about one's finances, health, race, ethnicity, shopping behavior, and geo-location to be combined with political interests, reading habits, and voting records. Social media and digital platforms are facilitating many of these techniques, monetizing and normalizing "fake news," "dark posts", and other practices, and challenging fundamental principles such as privacy, data protection, and individual autonomy. It has been widely reported that political Big Data digital micro-targeting played a role in the election of President Trump as well as the Brexit vote

in the UK, and is not the subject to growing scrutiny by regulatory authorities.

- Is the use of profiling technologies in political campaigns likely to influence voter preferences and undermine the democratic process? What is the link between these technologies and fake news?
- How do policy frameworks in western democracies compare, in terms of controlling political election campaigns practices?
- What is the role of data protection legislation in protecting the privacy of voters? And what are the challenges for data protection authorities in addressing how commercial data can be sold or shared with political groups?

#### 10:00 - Coffee break in Lounge Area 42

### 10:30 - DPAs AND NGOS: OPPONENTS OR ALLIES?

**Academic .. Policy .. Business ..**

**Organised by** CPDP

**Chair** Charles Raab, University of Edinburgh (UK)

**Moderator** Ivan Szekely, Central European University (HU)

**Speakers** Willem Debeuckelaere, Belgian Privacy Commission (BE), Fanny Hidvegi, Access Now (BE), Peter Schaar, European Academy for Freedom of Information and Data Protection (DE), Katarzyna Szymielewicz, Panoptykon Foundation (PL)

Over many years, Data Protection Authorities have experienced a variety of relationships with privacy and human rights NGOs. These relationships have ranged from hostility and criticism to collaboration and mutual assis-

tance. Sometimes NGOs have complained that DPAs are too unwilling to use strict enforcement and sanctions against organisations in breach of data protection law, and that they are not active enough against threats to information privacy rights. At other times, they have supported DPAs in efforts to raise public awareness and to require data controllers to be more transparent, accountable and compliant.

- How would you describe your relationships and experiences with the other kind of organisation?
- What criticisms would you make of the other kind of organisation?
- If your relationships are not satisfactory, how could they be improved, and will the GDPR provide new opportunities for collaboration?

#### 11:45 - THE FUTURE OF DATA PROTECTION ENFORCEMENT: WHAT TO EXPECT AND HOW TO PREPARE

**Academic • Policy • Business •••**

**Organised by** Wilson Sonsini Goodrich & Rosati (WSGR)

**Chair** Gwendal Le Grand, CNIL (FR)

**Moderator** Laura De Boel, WSGR (BE)

**Speakers** Caroline Louveaux, Mastercard (BE), Karolina Mojzesowicz, DG Just (EU), Romain Robert, EDPS (EU), Sachiko Scheuing, Acxiom (DE)

The GDPR and proposed ePrivacy Regulation introduce a new data protection enforcement regime in the EU. The panel will explain the new rules and discuss what businesses should expect and how they can get prepared. In particular, the panel will consider cross-border enforcement issues, the role of the European Data Protection Board, and the “one stop shop” mechanism. The panel will also analyze

regulators’ priorities and agenda and discuss current trends in enforcement actions.

- Should businesses prepare for high fines?
- How will DPAs handle cross-border enforcement?
- What will be the role of the European Data Protection Board? Can businesses take advantage of the “one stop shop” mechanism?

#### 13:00 - Lunch in Lounge Area 42

#### 14:15 - AUTOMATED DECISION-MAKING IN COMMERCIAL HEALTH

**Academic • Policy • Business •••**

**Organised by** Centre for Democracy and Technology

**Chair** Irina Vasilu, DG Just (EU)

**Moderator** Michelle De Mooy, Center for Democracy & Technology (US)

**Speakers** Michat Jan Boni, MEP (EU), Claire Gayrel, EDPS (EU), Finn Myrstad, Norwegian Consumer Council (NO), Irina Shklovski, IT University of Copenhagen (DK)

A large swath of personal health data in the commercial environment is governed by the “terms and conditions” set forth by companies, rather than by any regulatory scheme. This new data is being shared, aggregated, and used to make decisions about an individual’s health and well being. Companies use automated processes, like data analytics, that harness statistics, algorithms, and other mathematical techniques to convert data into actionable knowledge. In the context of health, automated systems like these may advocate for one course of medication or treatment over another. These systems also influence consumer health in more subtle ways by mediating behavior, such as through the exercise recommendations, ac-

cess to information, and search results for a health condition.

- How are health data collected, shared, and used in commercial apps?
- What types of analytics models are used to generate recommendations for individuals?
- How does bias impact different populations and developments in the market?

#### 15:30 - Coffee break in Lounge Area 42

#### 16:00 - THE CONNECTED HEALTH MARKETPLACE: ENSURING PRIVACY, SECURITY, AND EQUITY IN AN EMERGING INTERNET-OF-THINGS ENVIRONMENT

**Academic • Policy • Business ••**

**Organised by** American University

**Chair** David Martin, BEUC (BE)

**Moderator** Kathryn Montgomery, American University (US)

**Speakers** Giuseppe D’Acquisto, Italian Data Protection Authority (IT), Anne Kristin, Norwegian Consumer Council (NO), Candace Martin, Apple (US), Marijn Sax, University of Amsterdam (NL)

Wearable fitness devices, biosensor-equipped clothing, and “ingestibles” could help people lose weight, get into better shape, reduce stress, and take more control of their health. But some of the very features that make these new tools so promising also raise serious concerns. As their use becomes more widespread, and as their functionalities become even more sophisticated, the extent and nature of data collection will be unprecedented. Many of the harms associated with the collection and processing of such data, moreover, are likely to affect disproportionately the most vulnerable people in our society, including

the sickest, the poorest, and those with the least education. This panel will provide an overview of the major features, key players, and trends that are shaping the new consumer-wearables marketplace, discussing how best to ensure privacy, security, and equity.

- What are the key safety and data issues raised by health wearable and other connected-health devices?
- What is the relationship – in Europe and the U.S. – between the consumer wearables market and the connected health marketplace?
- How well do the GDPR and the new ePrivacy Directive provide safeguards for protecting consumer privacy and safety when using wearable devices?

#### 17:15 - THE INTERNET OF (VULNERABLE) BODIES

**Academic • Policy • Business ••**

**Organised by** Northeastern University and University of Ottawa

**Chair** Abigail Slater, Internet Association (US)

**Moderator** Andrea Matwyshyn, Northeastern University School of Law (US)

**Speakers** Jennifer Chandler, University of Ottawa School of Law (CA), Jens Clausen, Pädagogische Hochschule Freiburg (DE), Achim Klabunde, EDPS (EU), Judith Rauhofer, University of Edinburgh (UK)

This panel will explore the legal, technical, and ethical dimensions of security and privacy risks of human bodies becoming connected to and reliant upon the Internet – the Internet of Bodies (IoB). It will discuss the IoB casestudy of legal responsibility for unintended injuries resulting from the use of neuroprosthetics and the ethical issues

surrounding the casestudy of neuroprosthetics, including issues of autonomy, data security and privacy, just distribution, and managing public expectations.

- Introduction to IoB and shifting security, privacy, functionality, interoperability and other risks as IoT devices become IoB devices
- Discussion of the technical state of the

art of medical security vulnerabilities in business context

- Legal analysis under US, UK, and EU law and policy insights for expected future regulatory directions of IoB

### 18.30 - Cocktail followed by EDPS, FPF and Qwant Panel on Privacy by Design in Le Village

## CPDP2018 PANELS AT AREA 42 PETIT

### 8:45 - BETWEEN THE HARBOR AND THE SHIELD: THE IMPLEMENTATION OF EU-US PRIVACY SHIELD AGREEMENT

**Academic • Policy • Business •**

**Organised by** CPDP

**Chair** Irene Kamara, Tilburg University (NL)

**Moderator** Joan Antokol, Park Legal LLC (US)

**Speakers** Laurent Lim, EDPS (EU), Carol Evrard, Stibbe (BE), Nora Ni Loideain, University of Cambridge (UK), William Malcolm, Google (UK)

The EU-US Privacy Shield agreement is a self-certifying mechanism enabling transfers of personal data from the EU to the US under the adequacy principle. However, certain US companies and industries are outside its scope and certain companies still certify under the old Safe Harbor agreement, which does not apply any more. Before the adequacy decision enters into force, organisations need to prepare for it, taking into account different requirements differ based on whether the US company functions as a data controller or a data processor. Additionally, the Privacy Shield – unlike

the previous Safe Harbor – gives individuals the option to exercise their data protection rights. The panel will address the steps organisations and individuals should take to exercise their rights, and to enable their exercise, respectively.

- How to perform a lawful cross-Atlantic transfer to a US-based controller?
- Which additional content should processor terms with a US processor contain?
- How to enable the exercise of individual rights under the Privacy Shield?

### 10:00 - Coffee break in Lounge Area 42

### 10:30 - IS EVERYTHING FINE WITH ADMINISTRATIVE FINES?

**Academic • Policy • Business •**

**Organised by** CPDP

**Chair** Leonardo Cervera Navas, EDPS (EU)

**Moderator** Ruth Boardman, Bird&Bird (UK)

**Speakers** Paul Nemitz, European Commission (EU), Ian Walden, Queen Mary University of London (UK), Dana Irina Jaedicke, Norwegian DPA (NO), Steve Eckersley, ICO (UK)

Articles 83 and 84 of the GDPR lay down the rules for imposing administrative fines for infringement. The fines must be effective, proportionate and dissuasive without a trade-off among the three criteria, and they must reflect the gravity of each individual case. They must be imposed according to EU and Member State law, which provides for appropriate processual safeguards, including effective judicial review and the right to a legal remedy. However, as the fines can be high, they could mean a disproportionate burden on the European data-driven industries, decreasing their competitiveness and innovativeness, as certain member states and stakeholders argued during the legislative procedure.

- Are DPAs under the regulation obliged to impose a fine in all cases?
- Is there a trade-off among effectiveness, proportionality and dissuasiveness – and if there is, how to best address it?
- Which criteria should the competent authority take into account when assessing the nature and the gravity of the infringement?

### 11:45 - PROCESSING PERSONAL DATA IN A WORKING ENVIRONMENT

**Academic • Policy • Business •**

**Organised by** CPDP

**Chair** Javier Ruiz, Open Rights Group (UK)

**Moderator** Inge Vanderreken, Allen & Overy (BE)

**Speakers** Willem Debeuckelaere, Belgian Privacy Commission (BE); Yung Shin Van Der Syde, Time.lex (BE); Marta Otto, University of Lodz (PL), Alessandro Mantelero, Polytechnic University of Turin (IT)

The WP29 recently issued an opinion on

data processing at work, dealing with legal grounds for the processing and the employees' corresponding rights. Since employers hold a position of power over the employees, the latter cannot, on principle, validly consent to data processing. Therefore, the employers must seek alternative legal basis for data processing. This panel will address, in specific terms, and from different perspectives, how employers can process data in a GDPR-compliant manner, balancing between efficient business practices and effective exercise of employees' rights. Additionally, member states may impose more specific rules for data processing at work, leading to possible regulatory competition.

- How to define legal grounds for data processing at work in different contexts?
- How to balance the freedom of expression online with ICT-monitoring at work?
- How to be prepared for May 2018?

### 13:00 - Lunch in Lounge Area 42

### 14:15 - BEYOND SNOWDEN: A SURVEILLANCE REFORM UPDATE

**Academic • Policy •**

**Organised by** Brown University

**Chair** Deborah Hurley, Brown University (US)

**Moderator** Gus Hosein, Privacy International (UK)

**Speakers** Jason Biros, US mission to the EU (US), Timothy Edgar, Brown University (US), Katitza Rodriguez, Electronic Frontier Foundation (US), Anne Roth, German Parliament's NSA Inquiry Committee (DE)

This panel will examine the reforms adopted in the more than four years since the disclosures of NSA mass surveillance programs



# Friday 26 January 2018

## CPDP2018 PANELS AT GRANDE HALLE

beginning in 2013. These include Presidential Policy Directive 28, the USA FREEDOM Act, and recent changes to the NSA's Prism and "upstream collection" surveillance programs. How do these compare to changes adopted by other countries with major signals intelligence operations, including Germany and the United Kingdom? What more should be done to reform mass surveillance practices to protect privacy, civil liberties and human rights?

**15:30 - Coffee break in Lounge Area 42**

**16:00 - EDPL YOUNG SCHOLAR AWARD**

**Academic .....**

**Organised by** EDPL

The Young Scholars Award (YSA), hosted by the European Data Protection Law Review (EDPL) in cooperation with CPDP, is given annually to outstanding emerging researchers in the field of privacy and data protection law.

During this panel session, the three best young academics will present their research and discuss it with the competition jury members and the audience.

The winner of the award will be revealed at a ceremony at the end of the YSA panel.

Bart van der Sloot (Tilburg University), Maja Brkan (Maastricht University), and Mark Cole (University of Luxembourg) will discuss the papers. Serge Gutwirth (VUB) will award the prize.

- Eike Gräf (Freie Universität Berlin) - 'When Automated Profiling Threatens Our Freedom: A Neo-Republican Perspective'
- Zarine Kharazian (College of William & Mary) - 'Yet Another French Exception: The Political Dimensions Of France's Support For The Digital Right To Be For-

gotten'

- Anne-Laure Philouze (College of Europe) - 'The EU-US Privacy Shield: Has Trust Been Restored?'

**17:15 - ACADEMIC SESSION 4: ON FUNDAMENTAL RIGHTS**

**Academic .....**

**Organised by** CPDP

The last Academic Session of CPDP2018 is dedicated to fundamental rights and to their essence, with a particular reference to data protection.

Moeller, Sant Ana Pereira, and Korff will start by discussing the PNR Directive and its fundamental rights implications.

Porcedda will tackle the essence of the fundamental right to personal data protection in the EU legal order.

Brkan will conclude the session by discussing the notion of 'essence' of fundamental rights in European law.

The session will be chaired by Prof. Serge Gutwirth (VUB).

- Carolin Moeller (Optimity Advisors), Hugo Sant Ana Pereira (Optimity Advisors) and Douwe Korff (London Metropolitan University) Are Algorithms The Future of Law Enforcement? The Consideration of Fundamental Rights in the PNR Directive
- Maria Grazia Porcedda (University of Leeds). On boundaries. Finding the essence of the right to the protection of personal data
- Maja Brkan (Maastricht University). The essence of fundamental rights in EU law: Data privacy as a knife that peeled the onion to its core

**18.30 - Cocktail followed by EDPS, FFP and Qwant Panel on Privacy by Design in Le Village**

COMPUTERS, PRIVACY & DATA PROTECTION

**8:45 - USER EMPOWERMENT TECHNOLOGIES FOR PRIVACY, REGULATION AND COMPLIANCE**

**Academic .. Policy .. Business ..**

**Organised by** Fordham University

**Chair** Ioulia Konstantinou, VUB (BE)

**Moderator** Christopher Docksey, formerly of EDPS (UK)

**Speakers** Kristina Irion, University of Amsterdam (NL), Florence Raynal, CNIL (FR), N. Cameron Russell, Fordham University (US), Thanasis Zigomitos, University of Piraeus (GR)

New types of privacy technologies that provide users with more control over personal information or that use natural language processing and machine learning are being developed to empower users and enable more effective privacy notice and choice. Some examples include a tool that identifies whether the data practices encoded within a mobile app actually conform to a set of privacy requirements drawn from the app's privacy policy, a method to score and test the level of ambiguity in a privacy policy, and a technology to extract users' choice options. These technologies can also be used by companies to facilitate privacy compliance. At the same time, these technologies can assist DPAs and other regulators to identify problematic areas for enforcement. Lastly, these technologies may be used as "Privacy Bridges" for international data flows. This panel will highlight some of these technologies and address key questions surrounding their value-added to privacy by design such as:

- What are some of the recently released and in-development privacy technologies for user empowerment?
- How can these technologies help companies comply with the GDPR and other privacy obligations?
- How might these technologies provide "Privacy Bridges" for international data flows?

**10:00 - Coffee break in Le Village**

**10:30 - ARTIFICIAL INTELLIGENCE AND ETHICS**

**Academic .. Policy .. Business ..**

**Organised by** Microsoft

**Chair** Mireille Hildebrandt, VUB (BE)

**Moderator** Julie Brill, Microsoft (US)

**Speakers** Jim Dratwa, European Commission (EU), Father Benanti, Gregorian University (IT), Rich Caruana, Microsoft (US), Brent Mittelstadt, University of Oxford (UK)

Artificial Intelligence is one of the key technologies that will not only change industry but will have a significant economical and societal impact. After many decades of relatively slow progress in the field of AI, recent major breakthroughs in big data, massive computing power and sophisticated algorithms, have delivered us to the threshold of a new era in which our world will be filled with devices that perceive, learn, reason, make recommendations, and even act on our behalf. However, change of this magnitude never comes without disruption or uncertainty. The challenges facing the designing of AI is to

get not just the intelligence right, but also the human qualities of emotion, ethics and empathy. This means addressing unintentional bias in the design of an AI system, as well as the potential for a lack of fairness when an AI system is used to make important decisions impacting people. The critical next step in the pursuit of AI is to agree on ethical and empathetic framework for its design. Our panel of academic, government, industry experts will explore specific approaches to AI governance.

- What are the main ethical challenges that humans will have to face with the growth of AI?
- How can concerns over bias or a lack of fairness be mitigated by developers? How can processes and tools be developed that, where appropriate, identify and rectify bias in the data used to train AI systems?
- What does a possible AI ethical framework look like?

#### 11.45 - 11.50 - CNIL-INRIA PRIVACY AWARD CEREMONY

**Organised by** CNIL and INRIA

The CNIL-Inria Privacy Award is given annually to the authors of a computer science paper that contributes to the improvement of privacy or the protection of personal data. The paper may describe a fundamental research result, a technical innovation or provide a state of the art of a privacy related area. It must be the result of work carried out, at least in part, in a research lab in the European Union and must be published in the two years preceding the opening of the competition.

The jury is chaired by Daniel Le Métayer (Inria) and consists of: Claude Castelluccia (Inria), Emiliano De Cristofaro (University College,

London), Josep Domingo-Ferrer, (Universitat Rovira i Virgili, UNESCO Chair in Data Privacy), Simone Fischer-Hübner (Karlstad University), Sébastien Gambs (Université du Québec à Montréal), Matthieu Grall (CNIL), Krishna Gummadu (Max Planck Institute), Jaap-Henk Hoepman (Radboud University Nijmegen), Gwendal Le Grand (CNIL), Yves-Alexandre de Montjoye (Imperial College, London).

#### 11:45 - NATIONAL SECURITY: A FREE LICENCE FOR GOVERNMENT SURVEILLANCE?

**Academic ... Policy ... Business ...**

**Organised by** Council of Bars and Law Societies of Europe

**Chair** Iain Mitchell, CCBE (BE)

**Moderator** Joseph Cannataci, UN Special Rapporteur on the Right to Privacy (INT)

**Speakers** Isabelle Falque-Pierrotin, CNIL (FR), Sophie in 't Veld, MEP (EU), Michiel Pestman, Prakken d'Oliveira (NL), H.J. de Groot, General Intelligence and Security Service of the Netherlands (NL)

As national security issues can involve high stakes, it is important to critically analyse arguments invoking national security as a justification for measures limiting citizen's rights, particularly, data protection. However, a universally accepted definition of national security does not exist. Both at international and national level the term is not adequately specified. As a result, data protection infringements based on national security reasons cannot be effectively reviewed in courts to ensure that they comply with a strict test of what is necessary and proportionate.

In this panel, policy makers, academics, lawyers and law enforcement specialists will debate if and how the notion of national security as a justification for surveillance measures can be better embedded in national

democratic systems, where a key element of constitutionality remains in the effective judicial control and supervision of government action.

- How do the different stakeholders understand the notion of national security, particularly in relation to government surveillance?
- Is it possible and desirable to define the notion of national security?
- What measures can be taken to avoid or limit abuses of the use of national security exceptions to restrict data protection rights?

#### 13:00 - Lunch in Le Village

#### 14:15 - PRIVATISATION OF PRIVACY: FREEDOM AND DEMOCRACY AND THE THREAT OF GLOBAL TECH MONOPOLIES

**Academic ... Policy ... Business ...**

**Organised by** British Institute of International and Comparative Law (BIICL)

**Chair** Barry Lynn, Open Markets Institute (US)

**Moderator** Orla Lynsky, LSE (UK)

**Speakers** Christian D'Cunha, EDPS (EU), Liza Lovdahl Gormsen, British Institute of International and Comparative Law and University of Manchester (UK), Lina Khan, Yale University (US), Maurice Stucke, University of Tennessee College of Law and The Konkurrenz Group (US)

A main goal of open and competitive markets is to distribute information in ways that empower citizens to make wise economic and political decisions. But a growing concern is that today's democracies face an unprecedented threat. A few immense corporations have captured control over key chokepoints in the political economy and over much of

the "data" citizens use to govern themselves and their communities. More disturbing, the concern is that these gatekeepers use their monopoly power and control over data to manipulate commerce, news, and ideas in ways that violate basic rights. This raises two questions. Must citizens act? And if so, how? This panel will examine these concerns, how citizens have used "antitrust" to master similar challenges in the past, and how antimonopoly tools may also help promote privacy and the marketplace of ideas.

- Are the products and services we receive in exchange for our personal data worth it? or should the terms for providing personal data be reconsidered?
- Is it time to break up some of today's global platforms which hold near monopoly power?
- Is antitrust as we know it failing? should the rules of the digital playing field be reconsidered?

#### 15:30 - Coffee break in Le Village

#### 16:00 - ENCRYPTION OF COMMUNICATIONS AND E-EVIDENCE: CASPAR BOWDEN POLITICAL PANEL

**Academic ... Policy ... Business ...**

**Organised by** CPDP

**Chair** Paul De Hert, VUB (BE)

**Moderator** Giovanni Butterelli, EDPS (EU)

**Speakers** Gail Kent, Facebook (UK), Bart Preneel, KU Leuven (BE), Jay Stanley, ACLU (US), Xavier Tracol, Eurojust (EU), Cecilia-Joanna Verkleij, DG Home (EU)

For a long time encryption of communications has been implemented as a means to keeping communication secure and confidential. New and advanced technologies offer both new encryption opportunities and

also possibilities to break and circumvent encryption, both by governments and hackers. On the legal side, there is a heated debate as to how governments could legally gain access to people's electronic communications with as few hurdles as possible. This debate has gained prominence with the recent terrorist attacks. Thus, encryption has become a multi-faceted concept, which is seen both as preserving the confidentiality of communications as a pivotal element of privacy and data protection, and at the same time as a potential limitation of security. This raises the following questions:

- What are the data protection requirements on interference with the confidentiality of communications? In how far is encryption a hindrance for the work of the law-enforcement authorities?

- How can we legally and technically achieve secure and confidential communications without putting the work of the law-enforcement authorities at a disadvantage?
- What other fundamental rights could be impacted by breaches of encryption?

#### 17.15 - CONCLUDING REMARKS BY PAUL DE HERT AND GIOVANNI BUTTARELLI

#### 17.30 - Cocktail sponsored by Privacy Salon in Le Village

## CPDP2018 PANELS AT PETITE HALLE

### 8:45 - "SMART PRIVACY" IN CRITICAL INFRASTRUCTURES

**Academic • Policy • Business •**

**Organised by** SUCCESS Project

**Chair** Alessandro Mantelero, Polytechnic University of Turin (IT)

**Moderator** Gianclaudio Malgieri, VUB (BE)

**Speakers** Michael John, European Network for Cyber Security (NL), Raphaël Gellert, Tilburg University (NL), Stephanie Mihail, DG CNECT (EU), Silvia De Conca, Tilburg University (NL), Dennis Hirsch, Ohio State University Moritz College of Law (US)

The protection of personal data and privacy is a key issue in the field of critical infrastructures. In particular, "smart grids", "smart me-

ters", "smart cars" and electric vehicles are at same time a great opportunity in terms of green development and energy efficiency, and a challenge in terms of protection of citizens, consumers, and "data subjects". The aim of this panel is to discuss the risks that these new infrastructures pose in terms of secret surveillance or cyber attacks, the techniques for empowering users in controllership and/or ownership of smart meter data, smart cities data and smart car data as well as the legal or technical safeguards for minimizing cyber-risks.

- How to empower users/consumers in smart critical infrastructures? Is Data Protection Impact Assessment effective?
- How to balance cyber-security with privacy

cy (considering both legal solutions and technological solutions)?

- Should the protection of individuals with respect to critical infrastructures (smart meters, smart cars, smart cities) be sector-specific or based on general solutions?

#### 10:00 - Coffee break in Le Village

### 10:30 - FILLING 'ACCOUNTABILITY HOLES' IN ALGORITHMIC NETWORKS

**Academic • Policy • Business •**

**Organised by** eLaw Centre for Law and Digital Technologies, Leiden University

**Chair** Gianclaudio Malgieri, VUB (BE)

**Moderator** Francien Dechesne, Leiden University (NL)

**Speakers** Kyle Erickson, Palantir (US), Lorena Jaume-Palasi, Algorithm Watch (DE), Frederike Kaltheuner, Privacy International (UK), Karolina La Fors, Leiden University (NL)

Algorithms are becoming part of our daily lives: at our desks, kitchens, streets, clothes, business and government relations. While being of great utility, these algorithms shape people's worldviews and steer their behaviors. However, few fora exist where actors can initiate accountability checks to prevent and remedy negative implications of algorithms for personal lives and society at large. This interdisciplinary panel discusses tools, mechanisms and implementation processes to improve accountability in algorithmic networks.

- What kind of 'tools' (legal, socio-technical, political, ethical, awareness raising) for stakeholders (system developers, data-analysts, -subjects, business managers, policy makers, etc.) can improve accountability in algorithmic networks?

- What lessons have we learned from existing practices, such as Facebook editorial and system alerts against filter bubbles and fake news; requesting explanations about data use in Google Deepmind; 'trade union apps' against unfairness due to profiling?
- How to implement accountability mechanisms for algorithms during design, use and after (adverse) implications?

### 11:45 - DATA PROTECTION CHALLENGES IN HUMANITARIAN ACTION

**Academic • Policy • Business •**

**Organised by** Brussels Privacy Hub

**Chair** Catherine Lennman, Swiss DPA (CH)

**Moderator** Vagelis Papakonstantinou, VUB (BE)

**Speakers** Alexander Beck, UNHCR (INT), Christopher Kuner, BPH (BE), Massimo Marelli, ICRC (INT), Ben Parker, IRIN (CH), Alexandrine Pirlot de Corbion, Privacy International (UK),

The collection and processing of personally-identifiable data is central to the work of organisations in the humanitarian sector to protect and deliver essential aid to hundreds of millions of vulnerable individuals. This requires humanitarian organizations to implement data protection in their work. Compliance with personal data protection standards requires consideration of the specific scope and purpose of humanitarian activities to provide for the urgent and basic needs of individuals, and to protect their rights. This panel will consider how the imperatives of data protection and humanitarian action can both be realized on a global scale, particularly in light of new technologies. In view of this background, the panel will consider questions such as the following:

- What legal standards should be used to implement data protection in humanitarian action across various legal systems?
- How can data protection be balanced against other rights and freedoms in humanitarian action?
- What are the implications of data protection laws for international organizations working in the humanitarian sector?

### 13:00 - Lunch in Le Village

### 14:15 - HOW CAN EUROPEAN PRIVACY RULES HELP FOSTER INNOVATION BASED ON PRIVACY-BY-DEFAULT PRINCIPLES?

**Academic • Policy • Business •**

**Organised by** Qwant

**Chair** Ronald Leenes, Tilburg University (NL)

**Moderator** Pat Walsh, Privacy Matters (UK)

**Speakers** Guillaume Champeau, Qwant (FR), Isabelle Chatelier, DG Just (EU), Ninja Marnau, Saarland University (DE), Matilda Sisatto, European Parliament (EU)

The panel will approach both the GDPR and proposed ePrivacy Regulation, with regards to the obligations they set regarding privacy by design and by default, and explore how European industry and regulators should see the EU data protection legislation as a chance to gain the trust of consumers around the world and consequently therefore to gain market share.

- How is innovation compatible with the legal obligations for data protection by design and by default?
- What are the opportunities and caveats behind art. 25 GDPR?
- Who should implement the principles: Controllers, manufacturers or both?

### 15:30 - Coffee break in Le Village

### 16:00 - PRIVACY, HEALTHCARE AND HUMAN-ROBOT INTERACTION

**Academic • Policy • Business •**

**Organised by** Queen Mary University of London

**Chair** Silvia de Conca, Tilburg University (NL)

**Moderator** Eduard Fosch Villaronga, Queen Mary University of London (UK)

**Speakers** Robin L. Pierce, Tilburg University (NL), Aida Ponce, European Trade Union Institute (BE), Aviva de Groot, Tilburg University (NL), Heike Felzmann, NUI Galway University (IE), Scott Robbins, TU Delft (NL)

The integration of cyber-physical robotic systems in healthcare settings is accelerating. The panel aims to have an open discussion on the ethical, legal and societal implications of the growing use of robots and artificial intelligence technologies in sensitive contexts such as healthcare. Typical examples of such systems include surgery robots, assistants, therapeutic and rehabilitation robots, and even sex robots for healthcare purposes. Different robot embodiments may challenge different types of privacy, e.g. exoskeletons might challenge bodily privacy whereas assistant robots may challenge behavioral privacy. Moreover, as these technological developments may raise other different types of issues, ranging from the autonomy suppression or human-human interaction decrease, there may be a need for (some forms of) regulation. The panel will explore new privacy, autonomy and dignity concerns concerning the use of robot and artificial intelligence technologies in healthcare applications and will explore potential solutions.

- The growing use of emotions in hu-

man-robot interaction for therapeutic and commercial purposes.

- Policy issues regarding privacy trade offs in the integration of robotics in healthcare.
- Legal implications of the use of cloud services in robotics and Robot-as-a-Service.

## CPDP2018 PANELS AT LA CAVE

### 8:45 - CODE OF CONDUCT FOR MEDICAL RESEARCH: A RESOURCE IN TURBULENT TIMES?

**Academic • Policy • Business •**

**Organised by** BBMRI-ERIC

**Chair** Michaela Th. Mayrhofer, BBMRI-ERIC (AT)

**Moderator** Annelies Debucquoy, Belgian Cancer Registry (BE)

**Speakers** Evert-Ben van Veen, Medlaw-consult (NL), Anastassia Negrouk, EORTC (BE), Alastair Kent, Ambassador, Genetic Alliance (UK), Speaker tbc

The GDPR was influenced by contingent political priorities that risked creating unwanted effects on health research. The final result is acceptable, but many issues related to health research remain unanswered. The Code of Conduct for Health Research, born from the collaboration of more than 90 research organisations, aims at filling the gaps, to guarantee data collection and sharing that enable and enhance health research while respecting patient/citizens' rights. Experts and stakeholders will discuss the Code, underlining its added value and suggesting amelioration/critiques to it. The audience will have the chance to engage

### 17:15 - CONCLUDING REMARKS BY PAUL DE HERT AND GIOVANNI BUTTARELLI IN GRANDE HALLE

### 17:30 - Cocktail sponsored by Privacy Salon in Le Village

with the panellist and Code's authors.

- Providing the audience with a brief account of the specific data protection needs of health research;
- Discussing the procedural aspects how to submit a code of conduct under the GDPR (Art. 40);
- Engaging in a dialogue with the audience about what the Code of Conduct for Health Research should contain for both patients/citizens and researchers.

### 10:00 - Coffee break

### 10:30 - BIOMETRIC SYSTEMS, LAW ENFORCEMENT AND BORDER CONTROL: CHALLENGES IN THE NEW DATA PROTECTION ERA

**Academic • Policy • Business •**

**Organised by** University of Groningen

**Chair** Bogdan Manolea, Association for Technology and Internet (RO)

**Moderator** Shara Monteleone, European Parliament (EU)

**Speakers** Catherine Jasserand, University of Groningen (NL), Kiran Bylappa Raja, Norwegian University of Science and Technology (NO), Caroline Goe-mans-Dorny, INTERPOL (INT), Evgeni



Moyakine, University of Groningen (NL)

In modern society, governments and businesses rely heavily on biometric characteristics to identify individuals. Fingerprints and speech patterns are two examples of sensitive personal information commonly used for biometric recognition. With the introduction of the new EU legislative framework on data protection, including the General Data Protection Regulation and the new Directive for the police and criminal justice sector, new standards are to be applied to the biometric systems processing fingerprints and speech patterns. This panel relies on the findings from two EU FP7 research projects developing biometric technologies for law enforcement and/or border control purposes. It will address the new rules of the EU data protection legal regime and illustrate the most prominent legal, ethical, and technological issues arising in this regard.

- How can biometric data be processed for identification (law enforcement) and verification (border control) purposes?
- What is the role of biometric data in law enforcement cooperation and what are the challenges faced by international organisations in this regard?
- What is the impact of the "data protection by design and by default" obligation on the development of biometric systems?

#### 11:45 - BIG DATA: FRIEND OR FOE FOR CONSUMERS AND COMPETITION POLICY?

**Academic • Policy ... Business ..**

**Organised by** Brussels Office of the UK Law Societies

**Chair** Rachel Bickler, Brussels Section of the Law Society of England and Wales (BE)

**Moderator** Jeremy Rollison, Microsoft (BE)

**Speakers** Nico van Eijk, University of Amsterdam (NL), Ralf Bendrath, Office of Jan Albrecht MEP (EU), Raegan MacDonald, Mozilla (BE), Cyril Ritter, DG Comp (EU)

The Digital Single Market has increased access for consumers to buy goods and access services online. With the digital economy comes a plethora of benefits; however, the rise of super-platforms may pose many legal and regulatory challenges, in particular, when data and algorithms are combined. This starts to change the dynamics of competition in order to maximise efficiency for companies. The use of algorithms and increased automation of online transactions also has consequences for the consumers.

- Are algorithms good for competition?
- To what extent and in what context can algorithms pose a risk?
- How should algorithms be viewed from a consumer protection perspective? Should they be treated with caution or praised for placing a universe of products and services at the fingertips of the consumer?

#### 13:00 - Lunch in Le Village

#### 14:15 - BODIES IN THE CLOUDS

**Academic • Policy ... Business ..**

**Organised by** Access Now

**Chair** Wendy Grossman, Independent Journalist (US)

**Moderator** Lucie Krahulcova, Access Now (BE)

**Speakers** Ana-Maria Fimin, DG CNECT (EU), Ailidh Callander, Privacy International (UK), Leonie Tanczer, PETRAS IoT Hub (UK), Chris Gow, CISCO (BE), Lukasz Olejnik, Security and Privacy Consultant (PL)

The pervasive nature of the Internet of Things in our day to day lives means that there is an increasingly detailed picture of each of us in the cloud. Who we are as people - our movements, preferences, habits, friends, family, memories and our personalities - are continuously uploaded and analyzed, but do they come with the same safeguards that our physical selves enjoy in the offline world? This panel will investigate the human rights aspect of IoT and what legal protections apply to our digital footprint. It will also delve into why (if at all), we treat the digital realm differently. We will investigate the ethics of the usage of IoT and its data in police investigations as well as the ever-increasing danger of ubiquitous surveillance.

- Tracking, profiling and cloud analytics - where are the human rights safeguards?
- IoT evidence as part of investigations; and what you can do if your toaster was wrong.
- What is the responsibility of industry, governments and users?

#### 15:30 - Coffee break in Le Village

#### 16:00 - ROUNDTABLE: DATA PROTECTION AND POLICE COOPERATION IN THE AFSJ: EFFECTIVE SAFEGUARDS AND SUPERVISION

**Academic .. Policy ....**

**Organised by** CPDP

**Chair** Nathalie Falot, Considerati (NL)

**Moderator** Vagelis Papakonstantinou, VUB (BE)

**Speakers** Juraj Sajfert, DG Just (EU), Joanna Kulesza, University of Lodz (PL), Anna Moscibroda, DG Just (EU), Jaroslaw Lottarski, DG Home (EU), Mario Guglielmetti, EDPS (EU), Daniel Drewer, EUROPOL (EU)

It is expected that with Directive 2016/680 on

data protection in the law-enforcement sector becoming applicable, the personal data processed by the Member State law enforcement authorities will improve and become harmonized. In parallel, the pending amendment of Regulation 45/2001 might place the data processing activities of EU institutions, bodies and agencies in the Area of Freedom, Security and Justice (AFSJ) and the information systems they work with under (stricter) EDPS Supervision. In fact, the new 2016 EUROPOL Regulation already places EUROPOL under EDPS supervision. However, at the same time, work has been going on towards enhancing the existing AFSJ information systems, e.g. SIS II, EURODAC, setting up new ones, e.g. EES and ETIAS and making them interoperable, which brings new dimension/challenges to personal data processing. In addition, more initiatives are taken in respect to data transfer outside the Union for law enforcement purposes. Thus, questions on the effectiveness of the data protection provisions, especially in terms of supervision and safeguards, are raised. The panel will focus on the following questions:

- What are the desired changes to the current data protection regime of the AFSJ agencies/institutions/bodies?
- What supervision challenges do enhanced and interoperable information systems raise?
- Are there effective safeguards when personal data is transferred outside the EU for law enforcement purposes? What are the gaps?

#### 17:15 - CONCLUDING REMARKS IN GRANDE HALLE

#### 17:30 - Cocktail sponsored by Privacy Salon in Le Village

## CPDP2018 PANELS AT AREA 42 GRAND

### 8:45 - ALGORITHMIC TRANSPARENCY AND ACCOUNTABILITY IN LAW ENFORCEMENT

**Academic ... Policy ... Business •**

**Organised by** VALCRI, DANTE and VICTORIA

**Chair** Anton Vedder, KU Leuven (BE)

**Moderator** Eva Schlehahn, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (DE)

**Speakers** Joachim Klerx, Austrian Institute of Technology (AT), Penny Duquenooy, Middlesex University (UK), Christian Wiese Svanberg, Danish National Police (DK), Erik Zouave, Swedish Defence Research Agency (SE),

As policing has become increasingly data-driven and technology-based, algorithms play a crucial role in making profiling and biometrics more effective. More than ever, personal data is collected from public fora, such as through CCTV or social media, to infer suspects' physical, physiological and behavioral characteristics. Moreover, investigations must also be accurate, unbiased, and just. We examine how European data protection law regulates police profiling and biometrics and how it impacts police algorithms and discrimination. In particular, we discuss to what extent the regulatory frameworks address the challenge of achieving algorithmic transparency and accountability and the measures law enforcement can take.

- How do the deployment of automated decision-making processes and profiling techniques within the law enforcement context challenge the fundamental rights of the data subjects involved, such as the right to data protection and the

right to a fair trial?

- How does Directive 2016/680 aim to address these challenges through the principles of algorithmic transparency and accountability, what are potential shortcomings?
- How can system developers and law enforcement agencies come up with creative solutions beyond the law in order to ensure transparency and accountability, whilst remaining cognizant of law enforcement needs?

### 10:00 - Coffee break in Lounge Area 42

### 10:30 - DATA PROTECTION LAW AS THE LAW OF EVERYTHING? HOW THE GDPR COPES WITH LIMITS

**Academic .... Policy • Business •**

**Organised by** Tilburg Institute for Law, Technology, and Society (TILT)

**Chair** Juraj Sajfert, DG Just (EU)

**Moderator** Lee Bygrave, NRCCL (NO)

**Speakers** Nadya Purtova, Tilburg University (NL), Brendan Van Alsenoy, Belgian Privacy Commission (BE), Claudia Quelle, Tilburg University (NL), Mariarosaria Taddeo, University of Oxford (UK)

Despite the many failings of data protection law, government and corporation alike rarely act in a regulatory void. The GDPR applies to any processing of personal data pursued by controllers. With data protection teetering on the edge of irrelevance and impossibility, these boundary-markers have been stretched to encompass almost everything that can be done with data. From profiling to business administration, the GDPR requires controllers to act in a fair and legitimate

manner. But does data protection law actually hit the proverbial mark, achieving its goal without over- or under-regulating data processing? This panel will discuss the main boundary concepts under the GDPR. More precisely, this panel will discuss the concept of personal data, the legal construction of controllership, the risk-based approach as an attempt to regulate "risky" areas, and the focus of data protection discourse on individual rights.

- What is the meaning of "personal data" as a boundary concept for data protection law and how does it suit the rationale of data protection?
- Does the legal concept of "controller", together with the related concepts of "processor" and "joint controller", place responsibility for data protection law with the right entities?
- Does the notion of "a risk to the rights and freedoms of individuals" limit the application of the GDPR in a meaningful manner?

### 11:45 - ETHICS, RIGHTS AND DATA MANAGEMENT IN THE DIGITAL POLICING REVOLUTION

**Academic ... Policy ... Business •**

**Organised by** CRISP

**Chair** William Webster, University of Sterling (UK)

**Moderator** Rosamunde van Brakel, VUB (BE)

**Speakers** Fanny Coudert, EDPS (BE), Pete Fussey, University of Essex (UK), Katerina Hadjimatheou, University of Warwick (UK), Christian Wiese Svanberg, Danish National Police (DK)

The application of digital technologies for security and policing purposes continue to stimulate significant debate. These debates

reveal the range and diversity of such practices and include the exploitation of large-scale data sets for spatio-temporal crime forecasting, mining social media content, video analytics and processing and novel applications of AI. Despite attention to these practices, empirical analysis of their operational contexts is rare. Drawing on academic, activist, practitioner and regulatory perspectives, this panel examines the range of privacy and ethical issues that arise in this new domain of information practices.

- How do we conceptualise and understand contemporary digital policing practices?
- What are the privacy issues which arise in the context of new forms of digital policing?
- What are the possibilities for transparency, oversight and regulation for the diversity of activities that fall under the label of digital policing?

### 13:00 - Lunch in Lounge Area 42

### 14:15 - EUROPEAN LARGE-SCALE INFORMATION SYSTEMS AND THE USE OF BIOMETRICS: FUNDAMENTAL RIGHTS IMPLICATIONS

**Academic • Policy ... Business •**

**Organised by** European Union Agency for Fundamental Rights (FRA)

**Chair** Sergio Carrera, CEPS (BE)

**Moderator** Diana Dimitrova, FIZ Karlsruhe (DE)

**Speakers** Ann-Charlotte Nygård, EU Fundamental Rights Agency (EU), Ciarán Carolan, European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) (EU), Viktoria Astrid Nyström, AE Nyströms Advokatbyrå (SE), Owe Langfeldt, EDPS (EU)

The present trend is to collect an increasing amount of personal data of third country nationals (TCNs), including biometrics, in EU information systems. Existing EU information systems are: the Schengen Information System

(SIS II) to aid police and border checks, Eurodac (European Dactyloscopy) to support the application of the Dublin Regulation, and the Visa Information System (VIS) for supporting the processing of visa applications. Planned systems are: the Entry-Exit System (EES) for registering third country nationals (TCNs) who travel in and out of the EU, the European Travel Information and Authorisation System (ETIAS) for conducting pre-border checks of TCNs and the European Criminal Records Information System specific for TCNs (ECRIS-TCN).

In addition, the EC has launched two proposals to make the existing and planned systems interoperable. The right to protection of personal data, but also other fundamental rights implications, both negative and positive, emerge:

- How to ensure that the right to information as a principle of good administration covers all purposes of the data processing?
- Decisions on the future of the person is taken based upon data included in the databases, what are the possibilities to rebut a false assumption of the authorities based on inaccurate data and to have such data corrected or deleted?
- What are the implications of the processing of data in EU IT-systems on the right to asylum, as well as the rights of the child?

15:30 - Coffee break in Lounge Area 42

## 16:00 - PATERNALISM

**Academic • Policy • Business •**

**Organised by** Vrije Universiteit Amsterdam

**Chair** Arno R. Lodder, SOLV lawyers Amsterdam (NL)

**Moderator** Tina van der Linden, Vrije Universiteit Amsterdam (NL)

**Speakers** Amber Sinha, The Centre for Internet and Society (IN), Orla Lynsky, London School of Economics (UK), Walter van Holst, EDRI member Vrijdschrift (NL), Minke Reijneveld, Utrecht University (NL)

Privacy advocates are easy targets for accusations of paternalism. If you really considered it, you would not give permission! You do have something to hide! Don't click okay blindly. Some state, e.g. Ann Cavoukian, that a paternalistic approach to data protection could weaken rather than strengthen privacy in the 21st century. The introduction of the much debated cookie notices seems a case in point. The rationale was that in particular tracking and tracing cookies would be regulated. However, the obligatory consent implies an almost limitless processing of personal data, instead of no longer being followed, we are followed by dozens of businesses after we give our consent for using a website or app. Still, privacy, and in the European Union even data protection, are fundamental rights. As such, it is the duty of government to protect its citizens in this respect and create safeguards. But how, and to what extent?

- What if people really don't care and want to give blanket permission? Should they be allowed to do so? Or should we protect themselves against their own folly?
- What role should dignity play: respecting autonomy, or protecting individuals?

COMPUTERS, PRIVACY & DATA PROTECTION

- Is paternalism really a bad thing? What if you do know what is good for the other person?

## 17:15 - CONCLUDING REMARKS

BY PAUL DE HERT AND  
GIOVANNI BUTTARELLI  
IN GRANDE HALLE

17:30 - Cocktail sponsored by Privacy  
Salon in Le Village

## CPDP2018 PANELS AT AREA 42 PETIT

### 8:45 - ONCE MORE INTO THE BREACH: NOTIFICATION OF PERSONAL DATA BREACH UNDER THE GDPR

**Academic • Policy • Business •**

**Organised by** CPDP

**Chair** Steward Dresner, Privacy Law & Business (UK)

**Moderator** Christos Velasco, ProtDataMx (MX)

**Speakers** Dina Kampouraki, EDPS (EU), Marc Vael, Esco (BE), Erik Valgaeren, Stibbe (BE), Oliver Vettermann, FIZ Karlsruhe (DE)

According to the GDPR, the data controller is required to adopt certain security measures in order to prevent such breaches. Nonetheless, in case of an eventual breach, the controller is required to notify the competent authority, and under certain con-

ditions, the data subject as well. The main criteria for notification are "as soon as the controller has become aware", and "high risks to the rights and freedoms of natural persons", respectively. As these criteria are vague in nature, it is not always clear when and who must be notified. Taking into account the recent opinion of the WP29, this panel will discuss the notification duties under the GDPR, their timing, *raison d'être* and risk mitigation.

- How to define the moment a controller becomes aware of the data breach?
- When to notify the competent supervisory authority, and when the data subject?
- How to address personal data breaches in the DPIA process, considering they do not refer to the same "high risk"?

## 10:00 - Coffee break in Lounge Area 42

10:30 - (SELF-)PORTRAIT IN PROFILE:  
PROFILING AND ITS EFFECTS  
ON DATA SUBJECTS IN THE  
LIGHT OF THE NEW GUIDELINES**Academic • Policy • Business •****Organised by** CPDP**Chair** Damian Clifford, KU Leuven (BE)**Moderator** Frederik Zuiderveen Borgesius, VUB (BE)**Speakers** Zsuzsanna Belenyessy, EDPS (EU), Marit Hansen, Data Protection Commissioner for Schleswig-Holstein (DE), Laurens Naudts, KU Leuven (BE), Sandra Wachter, University of Oxford (UK)

Individual profiling with the goal of either categorising or predicting people's behaviour or other personal aspects is a given in today's digital economy. For businesses, it brings efficiencies, cost reductions and more customer-targeted services. However, it also carries certain risks, such as stigmatisation or knowledge asymmetries. The GDPR explicitly addresses such risks, and the WP29's recent guidelines provide more clarity on the subject. This panel will discuss how to implement the guidelines in practice from different points of view within different industries. Further, the relevance of human intervention and how risks, associated with profiling, are addressed in practice, taking into account different stakeholders (consumers, businesses, law enforcement, job candidates etc.).

- How to ensure appropriate exercise of data subjects' rights (right to an explanation, right to information etc.) vis-à-vis the profiler?
- Which are the best practices or implementing mitigation strategies?

- Do those mitigation strategies address privacy risks, such as stigmatization and knowledge asymmetries, and if not, which are the best practices to address such risks?

## 11:45 - DEEP IMPACT: THE OBLIGATION TO CARRY OUT A DPIA AND THE 'HIGH RISK' CRITERION

**Academic • Policy • Business •****Organised by** CPDP**Chair** Jos Dumortier, time.lex (BE)**Moderator** Michael Friedewald, Fraunhofer ISI (DE)**Speakers** Antoine Bon, Belgian Privacy Commission (BE), Paul Breitbarth, Nymity (NL), Ioana Cotoi, Engineering Ingegneria Informatica (IT), Paolo Sinibaldi, European Investment Fund (EU)

The Data Protection Impact Assessment (DPIA) describes the processing operation and assesses its necessity and proportionality as means of demonstrating GDPR compliance. A DPIA is required if the processing poses 'high risk' to individuals' rights and freedoms, if specifically set down in the GDPR or listed by the competent authority, whose perspectives will be discussed during this panel. The discussion will also focus on the main challenges organisations will face when carrying out the DPIA in terms of business processes, i.e. how to integrate the DPIA into the organisation's daily functioning, the review processes, and identifying the necessity of carrying it out. Further, the panel will consider the methods of risk management for DPIA purposes. The last question is when (and how much) to disclose the DPIA publicly, but taking into account the fact that it may contain security or commercially sensitive information.

- How and when to carry out a DPIA as part of the business and organizational process and how to identify high risks?
- Which are the best practices for choosing the methodology of DPIA as a risk-management exercise?
- When and why should data controllers make their DPIA public?

## 13:00 - Lunch in Lounge Area 42

14:15 - CYBERNETICS BETWEEN  
UTOPIA AND LOSS OF CONTROL.  
MANAGING TRANSPARENCY  
AND ACCOUNTABILITY OF  
ALGORITHMS THROUGH  
SOURCE CODE?**Academic • Policy • Business •****Organised by** Praemandatum**Chair** Daniel Guagnin, praemandatum (DE)**Moderator** Ben Wagner, WU Vienna (AT)**Speakers** Francien Dechesne, Leiden University (NL), Polina Malaja, Free Software Foundation Europe (DE), Mirco Pietsch, praemandatum (DE), Sandra Wachter, University of Oxford (UK)

Recently the debate about the power of algorithms has received more and more attention. Their shaping influence on society has become increasingly visible through selecting information in news and social networks. At the same time the dream of controlling society for the good is still hegemonic.

The utopia of cybernetics is not new, such is the criticism of the power of those who control the algorithms, which has been put forward by the early Free Software Movement in the Seventies. Beyond the efforts to regulate algorithms, we want to discuss different approaches of how to enable transparency and control of algorithms. For

end-users who cannot read source code, Free Software shifts the trust from a commercial company to a community of developers. This opens new levels of transparency and control, but should be complemented by ways to understand the functionality and data flows on a user level. The idea of putting control over algorithms into the hand of the users brings different challenges.

The panel brings together different perspectives: companies experimenting with open licenses, privacy scholars and software freedom activists to discuss the potential and the limitations of opening up the source code and other approaches for public scrutiny and control of algorithms.

- Which accountability does the source code provide?
- How can we make data flows, underlying norms and inscribed logics of algorithms visible?
- How can we empower users to take control and achieve transparency beyond the source code?

## 15:30 - Coffee break in Lounge Area 42

17:15 - CONCLUDING REMARKS  
BY PAUL DE HERT AND  
GIOVANNI BUTTARELLI  
IN GRANDE HALLE17:30 - Cocktail sponsored by Privacy  
Salon in Le Village



# CPDP2018 Side Events

## WED 24 JAN 2018

### **MALWARE, HACKING AND DATA LEAKS • A DISCUSSION ABOUT THE CURRENT STATE OF CYBERSECURITY**

**Organised by** Privacy Salon, deBuren, LSEC

**Date:** Wednesday 24 January 2018, 19:30

**Location:** deBuren, Leopoldstraat 6, Brussels

**Registration:** via [www.deburen.eu](http://www.deburen.eu)

Information technologies have transformed the way we live, work and divert ourselves. With these technologies come new threats to our security, from (sensitive) data leaks to virtual identity theft to cyber-espionage and viruses that can crash whole computer systems. In 2017, Europe was facing about 4000 ransomware attacks per day. It was also the year of yet another series of malware attacks targeting entities in public health, banking, communication, logistics, politics, etc. Cyberattacks are directed more increasingly towards government agencies and citizens. Some efforts to tackle such cyberattacks are taken on governmental level through strengthening of cybersecurity centres. But to what extent is this enough? Should citizens, organisations and companies be responsible for their own 'cyberhygiene' or should this be regulated and enforced by the EU or national governments?

### **A PRIVACYTOPIA event organised in the context of CPDP2018**

#### **20.20 - PECHA KUCHA**

**Organised by** Architempo & Privacy Salon

**Date** Wednesday 24 January 2018, 20:20

**Location** Les Halles de Schaerbeek, La Cave, Rue Royale-Sainte-Marie 22, 1030 Brussels

**Registration** [pechakucha.architempo.net](http://pechakucha.architempo.net)

**What?** 10 speakers, each speaker has 6 minutes 40 seconds for a presentation in 20 images. Each image is on screen for only 20 seconds. No more, no less. 20 images x 20 seconds each. Tempo, story, tension, show-and-tell. The Brussels format includes designers, architects, artists, scientists, fashion designers, photographers, musicians... Many will discuss technology and its implications. Some will not.

### **A PRIVACYTOPIA event organised in the context of CPDP2018**

#### **MOVE IT FORWARD FOR WOMEN'S HEALTH & BIG DATA - FEMALE DIGITAL STARTERS**

**This is a registration-only event.** The public is invited to the closing plenary, including project presentations and awards, which will take place on 25 January 2018 at 18.00.

**Organised by** Digital Leadership Institute and Privacy Salon

**Location** Area42, Rue de Palais 42-46, 1030 Brussels

**Dates** 24-25 January 2018

Privacy Salon, Digital Leadership Institute and its partners are proud to announce a FREE Move It Forward - female digital starters event for Women's Health & Big Data.

This initiative of the Digital Bruxelles female digital accelerator is supported by top technology companies, non-profit organisations, and youth and women's networks and communities. Its objective is to give teen and adult women the skills to become digital entrepreneurs and leaders, and to support them in driving positive change in their communities.

## THU 25 JAN 2018

### **MINI DESIGN JAM: CROSS-INDUSTRY SPRINTS FOR PRIVACY BY DESIGN**

**Organised by** Facebook

**Date** Thursday 25th January 14:15-15:45

**Location** Area42, Rue de Palais 42-46

To seize the opportunities of data, people need to feel in control of how it is used online. To give people real control you have to start with design. Every day, intuitive technologies are being designed that require no user training. We need to take the same approach to helping people understand how and why their data is used and putting them in control. Over the last year, along with partners, Facebook has piloted a unique programme called "Design Jam". The sessions bring together diverse experts, from regulators to behavioural scientists, to learn about design thinking – the methods used by designers to make technology usable and our lives simpler. At this 90-minute Mini Design Jam, participants will hear insights gleaned from the first events, learn about our vision for the future and even take part in a design experience of their own using a guided design method to understand a user and implement their design for an app.

### **PRIVACY BY DESIGN, PRIVACY ENGINEERING**

**Organised by** EDPS and supported by FPF and Qwant

**Date** Thursday 25 January 2018, 19:30

(preceded by a cocktail at 18:30)

**Place** Grande Halle, Halles de Schaerbeek

Introduction: Achim Klabunde, EDPS

**Moderator** Ninja Marnau, Senior Research-

er at the Center for IT Security, Privacy & Accountability, Saarland University, Saarbrücken  
**Speakers** Giovanni Buttarelli, EDPS, Jules Polonetsky, CEO, Future of Privacy Forum, Marit Hansen, Data Protection Commissioner, ULD Schleswig-Holstein, Eric Léandri, Co-founder and CEO Qwant

The GDPR introduces the obligation of data protection by design and by default. This is a very important step ahead and a challenge for many organisations, but it cannot be the end of the road.

For technology to serve humans, a broader view on privacy and ethical principles must be taken into account in its design and development.

The panel will discuss the perspectives of businesses and regulators which are the principles that they see as important in this context, and which are the approaches of their own organisations, and their demands and recommendations for other stakeholders.

### **DFF LAUNCH PARTY @CPDP**

CPDP is hosting the launch party of the Digital Freedom Fund, a new organisation that supports strategic litigation on digital rights in Europe.

**Join us for food, drinks and music to celebrate after a full day of engaging CPDP sessions.**

**When** 25 January, 19:30 – midnight

**Where** Area 42, 42 Rue de Palais

**No RSVP is required.**

**The event is kindly sponsored by Mozilla.**

FRI 26 JAN 2018

### ALGORITHMS AND COMPUTATIONAL PROPAGANDA IN SOCIAL MEDIA – DO WE HAVE ENOUGH DATA TO START POLICY DEBATE?

**Organised by** Panoptykon Foundation

**Speakers** Katarzyna Szymielewicz (Panoptykon Foundation), Paul-Olivier Dehaye (personaldata.io), Kristina Irion (IViR/UVA), Joris van Hoboken (UVA)

**Moderator** Anna Mazgal (Wikimedia Deutschland)

**Date** Friday 26 January 2018, 10:00-11:30

**Location** Area42, Rue de Palais 42-46

**The event is open to CPDP badge-holders only.**

The use of intransparent algorithms by online platforms to filter content shown to users has been framed as a problem requiring regulatory response. Many argue the 'filter bubble effect' limits users' access to information and exposure to different opinions and may have negative implications for political debate – including polarization and radicalization. However, there is little research on how filter bubbles are shaped. Which factors and agents determine what users see? Can commercial algorithms be manipulated? Can interventions have impact on political debate? What should be the response of companies and regulators? What is the role of data protection and DPAs regarding transparency and accountability? We will explore these questions with researchers and policy experts dealing with the mechanisms behind computational propaganda. Panoptykon Foundation will also present the results of research carried out in cooperation with the University

of Pennsylvania on filter bubbles and their impact on the Polish political debate.

SAT 27 JAN 2018

### PLSC-EUROPE

**Organised by** Privacy Salon and LSTS

**Date** 27 January 2018 at 08:30-18:30

**Location** Area 42, Rue de Palais 42-46

**More information and registration**

[www.cdpdconferences.org/plsc.html](http://www.cdpdconferences.org/plsc.html)

Based on the popular Privacy Law Scholars Conference (PLSC) event in the United States, PLSC-Europe is dedicated to bringing together privacy law scholars, practitioners, and privacy scholars from other disciplines from across Europe and beyond to discuss current issues. PLSC-Europe aims at fostering greater connections between academia and practice (industry, legal, advocacy, and government), and at bringing together law scholars with academics and professionals from other disciplines (e.g. economics, philosophy, political science, computer science). The first PLSC-Europe was held in October 2015 in conjunction with the Amsterdam Privacy Conference, and the second one in May 2017, in conjunction with TILting Perspectives 2017. From 2017 onwards, PLSC-Europe became a regular event co-organized by the University of Amsterdam (IViR), Tilburg University (TILT), and the Free University Brussels (LSTS/Privacy Salon), alternating between Amsterdam, Tilburg, and Brussels.

## Exhibitions

### WATCHING YOU, WATCHING ME – A PHOTOGRAPHIC RESPONSE TO SURVEILLANCE

**Curators** Stuart Alexander, Susan Meiselas, Yukiko Yamagata

**Opening** 25 January 2018 at 19.00, followed by two roundtable discussions

**Organised by** Open Society Foundations - New York

**In cooperation** with Privacy Salon and Bozar

**Dates** 25 January – 18 February 2018 (closed on Mondays)

**Location** Bozar, Centre for Fine Arts, Rue Ravensteinstraat 23, 1000 Brussels

**Image** © Julian Roeder

Watching You, Watching Me explores the intersection between photography and surveillance. Employing a dynamic range of approaches—from documentary to conceptual practice, from appropriation to street art—10 artists provide a satellite-to-street view of the ways in which surveillance culture blurs the boundaries between the private and public realm.

The exhibition looks into how photography can be both an instrument of surveillance and a tool to expose and challenge its negative impact. In tackling the inherent difficulty of visualizing something that is meant to be both omnipresent and covert—seemingly everywhere and nowhere at the same time—the artists in this exhibition employ a dynamic range of approaches.

With works by Mari Bastashevski & Privacy International, Edu Bayer, Josh Begley, Paolo Cirio, Hasan Elahi, Andrew Hammerand, Mishka Henner, Simon Menner, Julian Roeder



and Tomas van Houtryve.

**The exhibition will open on 25 January 2018, at 19:00** with two roundtable discussions presented by STAL - Sciences, Technologies, Arts, Lab - an initiative of BOZAR, VUB and ULB -, CPDP and Privacy Salon. Two of the artists - Julian Roeder and Mari Bastashevski - will each host a roundtable discussion with maximum 10 participants from different disciplines and sectors. Visitors to the expo can walk by, listen in and stay or move on.

**A PRIVACYTOPIA event organised in the context of CPDP2018**

## GLASS ROOM EXPERIENCE

**Organised by** Tactical Technology Collective and Mozilla

**Supported by** Privacy Salon and Muntpunt

**Dates** 9-27 January 2018

**Location** Muntpunt, Munt 6, 1000 Brussels

Do you feel like your digital self is slipping out of control? Have you let yourself install too many apps, clicked "I agree" a few too many times.

Following the amazing success of the The Glass Room exhibitions in New York and London, a smaller version The Glass Room is brought to Brussels at the invitation of Privacy Salon. It seeks to both expose and demystify how the largest data companies in the

world operate and what their relationship is with the individuals who they serve and on whom they depend. On Wednesdays and Thursdays afternoon, visitors are welcome to interact with our Data Detox Barista's and pick up their own 8-day Data Detox Kit.

**Guided tours** - every Wednesday afternoon.

**Guided tour & Disrupting Your Digital Shadow workshop Organised by** the Tactical Technology collective at the invitation of Privacy Salon - 20 January 2018 at 15:00

**Gluon workshop** - 27 January 2018 at 14:00

**A PRIVACYTOPIA event organised in the context of CPDP2018**

## PAINTED BY NUMBERS

### A DISCURSIVE INSTALLATION ON ALGORITHMIC REGIMES

**Concept and realization by** Konrad Becker and Felix Stalder, World-Information Institute

**Supported by** Privacy Salon

**Dates** 24-26 January 2018

**Location** Area42, Rue de Palais 42-46, 1030 Brussels

At the center of Painted by Numbers are artists, scientists, and activists who provide different perspectives on new algorithmic realities: are algorithms truly rational or do we only perceive them as such? Do they lack transparency? Are algorithms already shaping our cognitive processes? Interview excerpts are arranged according to theme in six channels: Rationality, Prediction, Agency, Regulation, Politics, and Culture, and visible

on six different screens. The interviewees' statements are not shown in a linear way, but create an open structure. This way, each viewer can choose an individual path in a cloud of overlaying audio and in a space of intersecting visual inputs.

The content is available as a spatial media installation, complemented by an online platform and offline events, which both function as discursive spaces. The outcome blends sociocultural debate and artistic media practice, exhibition and discourse spaces.

**A discussion with Mireille Hildebrandt, Seda Gurses, Felix Stalder and Konrad Becker will take place in Area42 on Friday 26 January at 16:00.**

**A PRIVACYTOPIA event organised in the context of CPDP2018**

## CPDP2018 Sponsors

### PLATINUM SPONSORS

# facebook

#### FACEBOOK

Founded in 2004, Facebook's mission is to give people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them.

# Google

#### GOOGLE

Google is a global technology leader focused on improving the ways people connect with information. Google's innovations in web search and advertising have made its website a top Internet property and its brand one of the most recognized in the world.

The logo for Huawei Europe, featuring a stylized red flower-like icon to the left of the text "HUAWEI EUROPE" in red capital letters.

#### HUAWEI

Huawei is a leading global information and communications technology (ICT) solutions provider. Our aim is to build a better connected world, acting as a responsible corporate citizen, innovative enabler for the information society, and collaborative con-

tributor to the industry. Huawei has over 9 900 staff based in Europe, of whom 1200 are working in R&D. We run 18 R&D sites located in eight European countries (Belgium, Finland, France, Germany, Ireland, Italy, Sweden and the UK) and operate numerous joint innovation centres in partnership with telecom and ICT partners. [www.huawei.eu](http://www.huawei.eu)

The Intel logo, consisting of the word "intel" in a blue, lowercase, sans-serif font, with a blue swoosh above the letters "l" and "e".

#### INTEL

Intel is the leading manufacturer of computer, networking and communications products. Intel develops semiconductor and software products for a range of computing applications. Headquartered in Santa Clara, California, it has 100,000 employees operating in 300 facilities in 50 countries. Intel's mission is to create and extend computing technology to connect and enrich the lives of every person on earth.

# les halles

#### LES HALLES DE SCHAEERBEEK

Ever since their beginnings, Les Halles have captured and crystallised movements stemming right from the edges of art and society, in an unprecedented alliance of both learned and popular culture. Open to contemporary hopes and upheavals spanning

from the neighborhood right out to the world at large, Les Halles keep on looking for what Europe, still on a quest for its own destiny, has to offer: exploration of new passions, reason seeking out adventure, the utmost freedom of style. Les Halles resonate with a desire for participation and involvement, be it individually or collectively, thus characterising the digital age.



#### MICROSOFT

Founded in 1975, Microsoft is the leading platform and productivity company for the mobile-first, cloud-first world, and its mission is to empower every person and every organization on the planet to achieve more. Our software innovations generate opportunities for the technology sector, businesses, public sector and consumers worldwide. Microsoft opened its first office in Europe in 1982. We have been investing in and growing with Europe ever since, and today we have over 25,000 local employees, working alongside more than 180,000 partners to empower millions of European consumers and to help transform businesses. In the last decade alone, Microsoft has invested nearly €20 billion in European companies, such as Nokia or Skype, as well as employed thousands of European researchers and engineers.



#### ONETRUST

OneTrust is the leading global software to operationalise data privacy compliance and Privacy by Design.

OneTrust automates data protection impact assessments (PIA) and data mapping, identifies privacy risks, and enforces risk management and control activities in an integrated and agile approach.

Our web-based software provides a central repository for privacy professionals to collaborate with business groups, service providers and trusted advisors managing privacy risks across controller, processor, and data transfer activities.

The result is the ability to demonstrate accountability and compliance with EU's data protection requirements (GDPR, BCR, Privacy Shield), and globally across privacy jurisdictions and frameworks.



#### TRUSTARC

Founded in 1997, TrustArc has evolved from a certification company into a global provider of technology powered privacy, data governance, compliance and risk management solutions. TrustArc provides integrated technology, consulting and TRUSTe certification solutions -- addressing all phases of privacy program management. The foundation for our solutions is the TrustArc Privacy Platform, which provides a flexible, scalable, and secure way to manage privacy, fortified through six years of operating experience across a wide range of companies and industry sectors. Headquartered in San Francisco, with offices in Europe and the Philippines, and backed by a global team, we help over 1,000 clients worldwide demonstrate compliance, minimize risk, and build trust. For more information, visit [www.trustarc.com](http://www.trustarc.com).

## PREMIER SPONSORS



#### APPLE INC.

Apple revolutionized personal technology with the introduction of the Macintosh in 1984. Today, Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch and Apple TV. Apple's four software platforms — iOS, macOS, watchOS and tvOS — provide seamless experiences across all Apple devices and empower people with breakthrough services including the App Store, Apple Music, Apple Pay and iCloud. Apple's more than 100,000 employees are dedicated to making the best products on earth, and to leaving the world better than we found it.



#### BSA | THE SOFTWARE ALLIANCE

BSA | The Software Alliance is the leading advocate for the global software industry. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC and operations in more than 60 countries around the world, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.



#### EUROPEAN COMMISSION DG-JRC

One of the missions of the Directorate E - Space, Security and Migration of the DG-JRC of the European Commission is to strengthen trust and security of the European Citizen in a sustainable and inclusive ICT-based European society by scientific research on how emerging Information and Communication Technologies will impact on the security and privacy of citizens' daily life. It works on risk mitigation, on cybersecurity, cybercrime, data protection, privacy and on the associated legal and regulatory frameworks aiming at a balance between European security needs and fundamental citizen rights including from the perspective of the emerging Digital Single Market.



#### EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

The European Data Protection Supervisor is an independent supervisory authority, with responsibility for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities at national level. The EDPS remit includes:

- developing and communicating an overall vision, thinking in global terms and proposing concrete recommendations;
- providing policy guidance to meet new



- challenges in the area of data protection;
  - operating at the highest levels and developing effective relationships with diverse stakeholders in other EU institutions, Member States, non EU countries and other national or international organisations.



### EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA)

The European Union Agency for Fundamental Rights (FRA), established by the EU as one of its specialised agencies in 2007, provides independent, evidence-based advice on fundamental rights to the institutions of the EU and the Member States on a range of issues. The staff of the FRA, which is based in Vienna, includes legal experts, political and social scientists, statisticians, and communication and networking experts.



### MOZILLA

Mozilla's mission is to promote openness, innovation and opportunity on the web. We produce the Firefox web browser and other products and services, together adopted by hundreds of millions individual internet users around the world. Mozilla is also a non-profit foundation that educates and empowers internet users to be the web's makers, not just its consumers. To accomplish this, Mozilla functions as a community of technologists, thinkers, and builders who

work together to keep the Internet alive and accessible. [www.mozilla.org/en-US/](http://www.mozilla.org/en-US/)



### QWANT

Designed and developed in France, Qwant is the first European search engine with its own indexing technology, which protects the privacy of its users by refusing all tracking devices, including for advertising. Contrary to the main search engines on the market, Qwant does not install cookies on the user browser, does not want to know who the user is or what he/she does, and does not keep individual logs of user queries.

Qwant's friendly interface allows users to find answers efficiently from the Web and social networks. It respects neutrality. Qwant considers all indexed websites and services with no discrimination, without altering the ranking of results according to its own interests.

Founded in 2013 by Eric Leandri, Jean-Manuel Rozan, Alberto Chalon and the Per-timm company, Qwant SAS has offices in Paris, Nice, Rouen, Ajaccio, Milan and Berlin. [www.qwant.com](http://www.qwant.com)

## EVENT SPONSORS



### DIGITAL FREEDOM FUND

The Digital Freedom Fund supports strategic litigation to advance digital rights in Europe. DFF provides financial support and seeks to catalyse collaboration between digital rights activists to enable people to exercise their human rights in digital and networked spaces.



### ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

EPIC is an independent non-profit research center in Washington, DC. EPIC protects privacy, freedom of expression, and democratic values; and promotes the Public Voice in decisions concerning the future of the Internet. EPIC's program activities include public education, litigation, and advocacy. EPIC files amicus briefs, pursues open government cases, defends consumer privacy, and testifies about emerging privacy and civil liberties issues. [www.epic.org](http://www.epic.org).



### FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a Washington, DC based think tank that seeks to advance responsible data practices. The forum is led by Internet privacy experts Jules

Polonetsky and Christopher Wolf and includes an advisory board comprised of leading figures from industry, academia, law and advocacy groups.



### HOGAN LOVELLS INTERNATIONAL LLP

Straight talking. Thinking around corners. Understanding and solving the problem before it becomes a problem. Performing as a team, no matter where we're sitting. Delivering clear and practical advice that gets your job done.

Our 2,500 lawyers work together, solving your toughest legal issues in major industries and commercial centers. Expanding into new markets, considering capital from new sources, or dealing with increasingly complex regulation or disputes - we help you stay on top of your risks and opportunities. Around the world.



### ISACA BELGIUM

ISACA Belgium is a non-profit knowledge chapter with +900 volunteers in Belgium and is part of ISACA international with +140.000 volunteers worldwide. ISACA is focused on IT auditing, IT governance, IT risk, information security, cybersecurity and privacy. ISACA Belgium organizes certification boot camps to prepare candidates for their CISA, CISM, CGEIT, CRISC and CSX exams. On average,

ISACA Belgium organizes more than 20 educational activities per year, including privacy open forums via [www.isaca.be](http://www.isaca.be). ISACA publishes regularly privacy white papers, articles and blogs by volunteers which can be found on [www.isaca.org/privacy](http://www.isaca.org/privacy)



## NYMITY

Nymity is a global research company specialising in accountability, risk, and compliance solutions for the privacy office. Nymity helps organisations attain, maintain, and demonstrate data privacy compliance, in all jurisdictions, industries, and sectors. Organisations all over the world rely on Nymity's solutions to proactively and effectively manage their privacy programs – empowering them to comply with confidence. Learn more at [www.NYMITY.com](http://www.NYMITY.com)

# Stibbe

## STIBBE

Stibbe's team of privacy and data protection specialists provides its clients with insight, foresight and experienced pragmatism. The team has over 20 years of experience in dealing with data protection authorities from different jurisdictions. The team is embedded in Stibbe's TMT practice (Technology Media and Telecoms), and, as a result, the members have a thorough understanding of information technology and data communication networks. The team is

involved in data governance protection projects for national and international clients, covering an a broad range sectors, such as media/entertainment, finance, communications, industry and transport, consumer goods, government and healthcare. Typical projects include privacy health checks, corporate data exchange and monitoring programs and policies. Click on the links for more information on our practice group and its publications.



## WILSON SONSINI GOODRICH & ROSATI

Wilson Sonsini Goodrich & Rosati is a global law firm that helps clients maintain the highest standards for data protection while successfully pursuing their business interests. We have a fully integrated global practice with substantial experience in advising companies on all facets of global and EU privacy laws, including on topics such as big data, connected cards, cloud computing, and the Internet of Things. We have unique experience with complex multi-jurisdictional privacy investigations, enforcement actions, and litigation. We also counsel clients on the review of the EU data protection legal framework. More information: [www.wsgr.com](http://www.wsgr.com) and WSGR Data Protection Regulation Observatory: [www.wsgr.com/eudataregulation](http://www.wsgr.com/eudataregulation)

## THANK YOU

This conference would not be possible without the industrious support of Els Vertriest and Laurence Schepens and all Medicongress staff, and the technical support of Olivier De Baere and his team at Create Live. Also for the mastery of our caterer KoKoen, thank you to Koen Devolder and his team for providing such delicious food! A big thank you to Christophe Galent and Anick Xhrouet for the great partnership between CPDP and Les Halles all these years and thank you to all the staff of Les Halles for making it possible to hold our event in one of the most famous and well reputed cultural centres in Brussels. Thank you very much to Fernand Van Bever and his team from Les Halles for making all this "technically" feasible. It's a kind of magic! To Samuel Wodinski – our tireless cameraman – whose relentless filming and photography will provide us with great visuals of the conference, the panels and the side events. To Lore Aerts for the continued logistical support for CPDP and side events. Many thanks also to the job students from the VUB and the volunteers from the TILT research group and elsewhere, who have done and are doing a wonderful job.

Special thanks to all people involved in organising the side events of CPDP. Especially a big thanks to Irina Baraliuc who coordinated and organised the great line up of side events including the art exhibitions, the workshops and the cybersecurity debate. Imge Ozcan, Kirsten Fiedler and Rocco Bellanova for organising a brilliant line-up for Privacy Camp. Alok Nandi (Architempo) for organising yet another fantastic Pecha Kucha! Amy Weatherburn, Laura Drechsler, Gloria González Fuster and Hielke Hijmans at the Brussels Privacy Hub who co-organised our launch event.

Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, the editors of the conference proceedings, which has now moved to Hart Publishing, did a great job again. As with every year, they have produced a book of high value which leaves written proof of what CPDP is: an ambitious bet to knock down barriers among disciplines, think together, innovate and leave a mark in the privacy and data protection world. Thank you also to our brilliant team of reviewers for the call for papers: Meg Ambrose, Jef Ausloos, Emre Bayamlıoglu, Gergely Biczók, Michael Birnhack, Damian Clifford, Colette Cuijpers, Lorenzo Dalla Corte, Silvia De Conca, Denis Duez, Michael Friedewald, Masa Galic, Raphael Gellert, Inge Graef, Serge Gutwirth, Marit Hansen, Irene Kamara, Els Kindt, Eleni Kosta, Ronald Leenes, Daniel Le Métayer, Alessandro Mantelero, Bryce Newell, Nóra Ni Loideain, Robin Pierce, Jo Pierson, Charles Raab, Arnold Roosendaal, Joseph Savirimuthu, Maurice Schellekens, Hosna Skeikhhattar, Ivan Skorvanek, Sophie Stalla-Bourdillon, Ivan Szekely, Mistale Taylor, Brendan Van Alsenoy, Bart van der Sloot, Yung Shin Van Der Sype, Joris van Hoboken, Bastiaan van Loenen, Gabriela Zanfir Fortuna, Nicolo Zingales and for the conference book: Meg Ambrose, Norberto Andrade, Rocco Bellanova, Colin Bennett, Bibi Van Den Berg, Michael Birnhack, Gabriela Bodea, Franziska Boehm, Jacquie Burkell, Mark Cole, Bart Custers, Lorenzo Dalla Corte, Els De Busser, Marieke de Goede, Denis Duez, Lillian Edwards, Michael Friedewald, Lothar Fritsch, Raphael Gellert, Gloria González Fuster, Nathalie Grandjean, Dara Hallinan, Marit Hansen, Natali Helberger, Joris van Hoboken, Chris Hoofnagle, Gerrit Hornung, Kristina Irion, Irene Kamara, Els Kindt, Eleni Kosta, Daniel Le Métayer, Arno R. Lodder, Orla Lynskey, Hiroshi Miyashita, Michael Nagenborg, Bryce Newell, Ugo Pagallo, Monica Palmirani, Jo Pierson, Bart Preneel, Nadezhda Purtova, Charles Raab, Antoni Roig, Arnold Roosendaal, Ira Rubinstein, Joseph Savirimuthu, Burkhard Schafer, Bart Van der Sloot, Ivan Szekely, Linnet Taylor, Mistale Taylor, Tjerk Timan, Peggy Valcke, William Webster, Tal Zarsky.

A special word of gratitude goes out to Nick Van Hee, our web-master and graphic designer, who has been with CPDP since the very beginning and even under great pressure always stays positive, someone with a hugely creative mind, a strenuous worker and authentic team player.

Last but not least, the Programming Committee of CPDP2018 would like to thank all sponsors, conference partners, event partners, moral supporters and media partners for their generous support and everyone who has approached us with new ideas and topics for panels. Without them CPDP2018 would not have been possible!