

12th INTERNATIONAL CONFERENCE 30 JAN - 1 FEB 2019 BRUSSELS, BELGIUM

CPDP DATA PROTECTION 2019 AND DEMOCRACY

WWW.CPDPCONFERENCES.ORG



INFO, PROGRAM & REGISTRATION: WWW.CPDPCONFERENCES.ORG

f www.facebook.com/CPDPconferencesBrussels t twitter.com/CPDPconferences

✉ info@cpdpconferences.org ▶ www.youtube.com/user/CPDPconferences

12th INTERNATIONAL CONFERENCE 30 JAN - 1 FEB 2019 BRUSSELS, BELGIUM

CPDP DATA PROTECTION 2019 AND DEMOCRACY



WWW.CPDPCONFERENCES.ORG

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 12th edition of CPDP! I hope many of you already enjoyed our pre-events including Privacy Camp and the CPDP opening night featuring the launch of Shoshana Zuboff's new book "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power".

This year's overarching theme is "Data Protection and Democracy", to pave the way for a timely and thorough discussion over a broad range of ethical, legal and policy issues related to new technologies and data analytics and to highlight data protection as a core element of a democratic society.

2019 has only just begun – what will the year hold for privacy and data protection? Over the past year, the GDPR came into effect, a major step forward with a potential for international impact. But is the GDPR the panacea for all the legal issues arising from an increasingly data-driven world? We are bringing you a couple of exciting panels seeking answers to such big questions. Our conference programme promises to provide many more engaging discussions with topics ranging from blockchain, cross-border access to e-evidence, Big Data in health care to data protection impact assessments, collective redress, privacy by design, data and elections, predictive policing, and much more.

Besides 3 days of panels across 6 stages, CPDP will also feature a range of exciting side events including artist talks on quantification, algorithms and facial recognition as well as our famous PechaKucha evening. And please join us for the official CPDP party on Thursday evening to blow off some steam after intense days of discovering, discussing and networking.

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

12th INTERNATIONAL CONFERENCE
30 JAN - 1 FEB 2019 📍 BRUSSELS, BELGIUM
COMPUTERS, PRIVACY
& DATA PROTECTION
CPDP2019
**DATA PROTECTION
AND DEMOCRACY**

CONTENTS

FOREWORD	3
GENERAL CONGRESS INFORMATION	7
ORGANISATION OF CPDP2019	9
CORE PROGRAMMING COMMITTEE	9
EXTENDED PROGRAMMING COMMITTEE	9
SCIENTIFIC COMMITTEE	9
MAP OF LES HALLES	11
RESTAURANTS CLOSE BY	11
CONFERENCE BOOKS	12
AWARD CEREMONIES AT CPDP2019	13
EPIC INTERNATIONAL PRIVACY CHAMPION AWARD	13
EDPL Young Scholar Award	13
CNIL-INRIA AWARD	13

CPDP2019 GRIDS

SEE SEPERATE BROCHURE

DATA PROTECTION AND DEMOCRACY

WEDNESDAY 30 JANUARY 2019

CPDP2019 PANELS AT GRANDE HALLE	14
CPDP2019 PANELS AT AREA 42 GRAND	18
CPDP2019 PANELS AT PETITE HALLE	22
CPDP2019 PANELS AT LA CAVE	26
CPDP2019 PANELS AT AREA 42 PETIT	30
CPDP2019 PANELS AT MAISON DES ARTS	33

THURSDAY 31 JANUARY 2019

CPDP2019 PANELS AT GRANDE HALLE	34
CPDP2019 PANELS AT AREA 42 GRAND	40
CPDP2019 PANELS AT PETITE HALLE	44
CPDP2019 PANELS AT LA CAVE	48
CPDP2019 PANELS AT AREA 42 PETIT	51

FRIDAY 1 FEBRUARY 2019

CPDP2019 PANELS AT GRANDE HALLE	55
CPDP2019 PANELS AT AREA 42 GRAND	58
CPDP2019 PANELS AT PETITE HALLE	61
CPDP2019 PANELS AT LA CAVE	64
CPDP2019 PANELS AT AREA 42 PETIT	67

CPDP2019 SIDE EVENTS

PRIVACYTOPIA ARTISTIC PROGRAMME	70
	72

CPDP2019 SPONSORS LOGOS

CPDP2019 SPONSORS	39
SEE SEPERATE BROCHURE	

CPDP2019 CONFERENCE PARTNERS	76
------------------------------	----

THANK YOU	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 booth. This booth is located in Le Village and is open on Wednesday and Thursday.

INTERNET LOGIN AND PASSWORD

Select SSID or Network: CPDP · Password: CPDP2019

VENUES

CPDP takes place simultaneously in two venues. Two tracks of sessions will take place at Area 42 Grand and Petit rooms. 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. There will be signposts and 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 bars in La Ruelle and in Area 42 stay 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.

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.

DATA PROTECTION AND DEMOCRACY

CHOOSE YOUR PRIVACY PREFERENCES AT CPDP 2019!

A professional photographer will be taking photos at the conference venues, including crowd shots, which then will be used for publicity. If you don't want to be photographed, please opt for an orange no-photo lanyard at the registration desk, and make sure to wear it visibly.

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

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 homepage: www.cpdpconferences.org and twitter [@cpdpconferences.org](https://twitter.com/cpdpconferences.org)

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.

Please get in touch if you have any issues with this via info@cpdpconferences.org or mention this at the registration desk.

Organisation of CPDP2019

- 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)
- Diana Dimitrova (FIZ Karlsruhe)
- Lorenzo Dalla Corte (Tilburg University TILT, TU Delft A+BE)
- Ioulia Konstantinou (Vrije Universiteit Brussel LSTS)

EXTENDED PROGRAMMING COMMITTEE

- Andrew Adams (Meiji University)
- Dennis Hirsch (Ohio State University Moritz College of Law)
- Ronald Leenes (Tilburg University TILT)
- Malavika Jayaram (Digital Asia Hub)
- Omer Tene (International Association of Privacy Professionals)

PANEL COORDINATORS

- István Böröcz (Vrije Universiteit Brussel LSTS)
- Eike Gräf (Vrije Universiteit Brussel LSTS)
- Irene Kamara (Tilburg University TILT, Vrije Universiteit Brussel LSTS)
- Gianclaudio Malgieri (Vrije Universiteit Brussel LSTS)
- Sara Roda (Vrije Universiteit Brussel LSTS)
- Deepan Sarma (Vrije Universiteit Brussel LSTS)
- Yung Shin Van Der Sype (KU Leuven, time.lex)

SCIENTIFIC COMMITTEE

- Rocco Bellanova, University of Amsterdam (NL)
- Franziska Boehm, Karlsruhe Institute of Technology, FIZ Karlsruhe – Leibniz Institute for Information Infrastructure (DE)
- Ian Brown, Research Ict Africa (Sa)
- Paul De Hert, Vrije Universiteit Brussel LSTS (BE), Tilburg University TILT (NL)
- Willem Debeuckelaere, Belgian Data Protection Authority (BE)

- Claudia Diaz, Katholieke Universiteit Leuven (BE)
- Denis Duez, Université Saint-Louis - Bruxelles (BE)
- Michael Friedewald, Fraunhofer Institut Für System- Und Innovationsforschung ISI (DE)
- Serge Gutwirth, Vrije Universiteit Brussel LSTS (BE)
- Marit Hansen, Independent Centre For Privacy Protection ULD (DE)
- Mireille Hildebrandt, Universiteit Nijmegen (NL) & Vrije Universiteit Brussel LSTS (BE)
- Dennis Hirsch, Ohio State University Moritz College of Law (US)
- Gus Hosein, Privacy International (UK)
- Kristina Irion, Marie Curie Fellow, Institute for Information Law IViR (NL)
- Els Kindt, Katholieke Universiteit Leuven Center for IT & IP Law (BE)
- Bert Jaap Koops, Tilburg Institute for Law, Technology, and Society TILT (NL)
- Eleni Kosta, Tilburg Institute for Law, Technology and Society TILT (NL)
- Daniel Le Métayer, Institut National de Recherche en Informatique et en Automatique INRIA (FR)
- Ronald Leenes, Tilburg Institute for Law, Technology and Society TILT (NL)
- Charles Raab, University of Edinburgh (UK)
- Marc Rotenberg, EPIC (US)
- Antoinette Rouvroy, University of Namur FUNDP, CRID (BE)
- Ivan Szekely, Central European University (HU)
- Frederik Zuiderveen Borgesius, Radboud University & IViR Institute for Information Law (NL)

LOGISTICS AND REGISTRATION



MediCongress Services

Noorwegenstraat 49 • 9940 Evergem
Belgium • Phone: +32 (0)9 218 85 85
www.medicongress.com

CREATE

CREATE

Noorwegenstraat 49 • 9940 Evergem
Belgium • T +32 (0) 9 330 22 90
www.create.eu • info@create.eu

LOGISTICS AND ADMINISTRATIVE SUPPORT

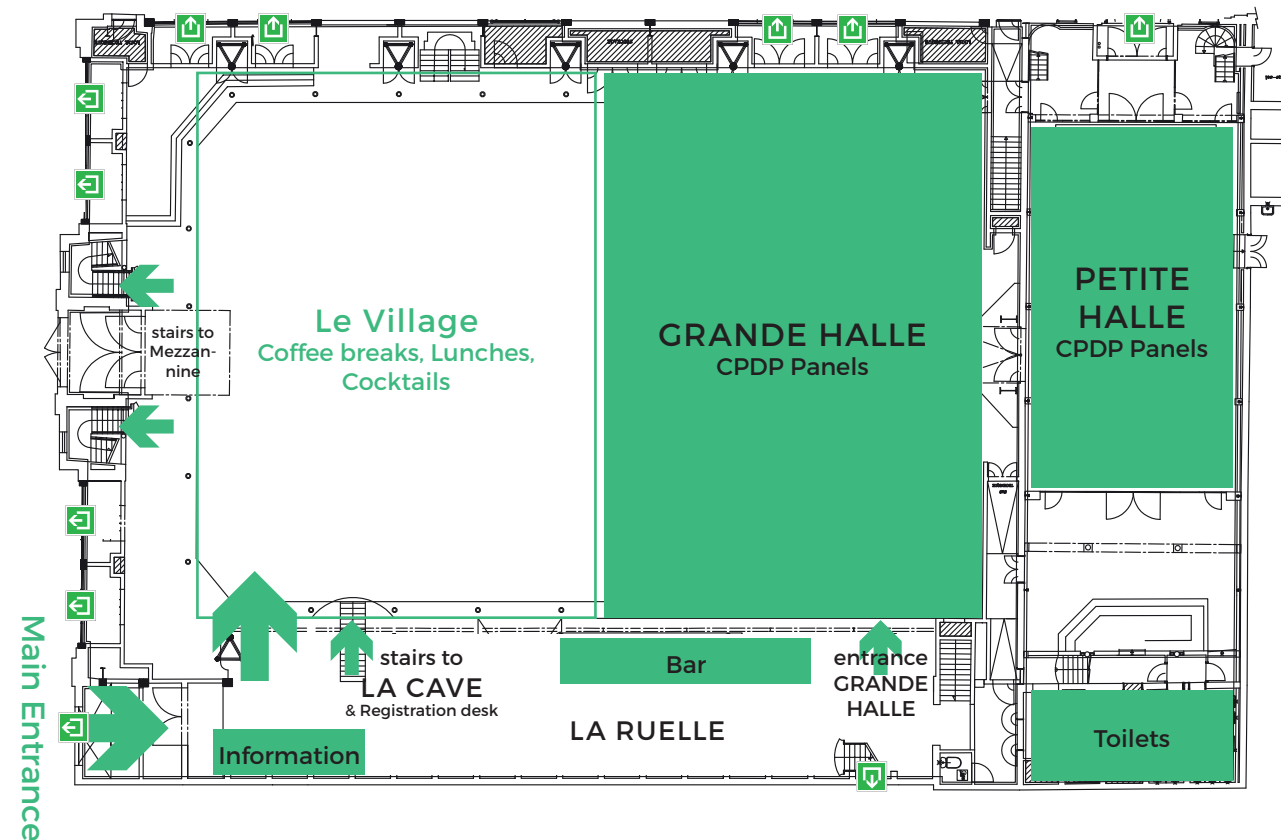


www.privacysalon.org

Design © Nick Van Hee – www.nickvanhee.be

COMPUTERS, PRIVACY & DATA PROTECTION

LES HALLES



RESTAURANTS CLOSE BY

- **Le Chambord** (Italian, Belgian) €€
Causée 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) €€€
Causée 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

DATA PROTECTION AND DEMOCRACY



CONFERENCE BOOKS

Books based on papers presented at previous CPDP conferences:

- Gutwirth, S., Pouillet, 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)
- Gutwirth, S., Pouillet, 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)
- Gutwirth, S., Pouillet, 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)
- Gutwirth, S., Leenes, R., De Hert, P. and Y. Pouillet, **European Data Protection: In Good Health?** Dordrecht: Springer, 2012. (www.springer.com/law/international/book/978-94-007-2902-5)
- Gutwirth, S., Leenes, R., De Hert, P. and Y. Pouillet, **European Data Protection: Coming of Age** Dordrecht: Springer, 2012. (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)
- 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)
- Gutwirth, S., Leenes, R. and P. De Hert, **Data Protection on the Move**, Dordrecht: Springer, 2016 (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/>)
- Leenes, R., Van Brakel, R., Gutwirth, S. and P. De Hert, **Data Protection and Privacy, Vol. 11, The Internet of Bodies**, Oxford: Hart Publishing, 2018 (<https://www.bloomsburyprofessional.com/uk/data-protection-and-privacy-9781509926206/>)

CPDP2019 Award Ceremonies

CNIL-INRIA 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 (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), Seda Gürses (KU Leuven), Gwendal Le Grand (CNIL), Yves-Alexandre de Montjoye (Imperial College, London).

The CNIL/INRIA Awardee(s) will present his/her/their paper Wednesday 30 at 16:00 in Area 42 Petit.

Award ceremony Wednesday 30 January 2019 at 14:15 in Grande Halle

EPIC INTERNATIONAL PRIVACY CHAMPION 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: Gus Hosein (2018), Artemi Rallo (2018), Alexander Dix (2017), Viviane Reding (2016), Peter Hustinx (2015), MEP Jan Philipp Albrecht (2014), Max Schrems (2013), Jennifer Stoddart (2012), MEP Sophie In't Veld (2011), Justice Michael Kirby (2010), Prof. Stefano Rodotà (2009).

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

Award ceremony Wednesday 30 January 2019 at 18:30 in Grande Halle

EDPL YOUNG SCHOLAR AWARD

The EDPL Young Scholar Award (YSA), now in its third edition, is an annual competition for outstanding research by Master and PhD students in the field of EU privacy and data protection law. Organised by the European Data Protection Law Review (EDPL), the competition includes a dedicated panel at CPDP (Thursday 31/01, 16:00, Area 42-petit) where the best three authors present their research and discuss it with the YSA jury (Bart van der Sloot, Maja Brkan, and Mark Cole) and the audience. The winner of the 3rd EDPL Young Scholar Award will be revealed at the panel and the award will be presented by Prof. Serge Gutwirth.

The top 5 articles of this year's YSA are available in issue 4/2018 of the EDPL journal.

Thursday 31 January 2019 at 16:00 in Area 42 Petit

DATA PROTECTION AND DEMOCRACY

WEDNESDAY 30TH JANUARY 2019

07:30 - Registration in La Cave

08:15 - Welcome coffee in Le Village

CPDP2019 PANELS AT GRANDE HALLE

08:30 - Welcome and Introduction by Paul De Hert in Grande Halle

8:45 – INFLUENCE OR MANIPULATION? WHAT PROTECTIONS IN THE DIGITAL WORLD?

Academic ** Business ** Policy **

Organised by Inria

Chair Daniel Le Métayer, Inria (FR)

Moderator Rocco Bellanova, UvA (NL)

Speakers Claude Castelluccia, Inria (FR), Bart Engelen, Tilburg University (NL), Fanny Hidvegi, Access Now (BE), Judith Möller, UvA (NL)

The digital world is prone to manipulation. Data do not just represent phenomena, but they also provide the means to act upon our world. Nowadays, the central role of digital data and their concentration in the hands of a few actors opens up new avenues for all sorts of manipulations. Some extreme cases have been highly publicized and widely discussed, in particular in the context of national elections. However, the precise role of the stakeholders involved and the impact of the manipulations are still not fully established. More fundamentally, the very definition of manipulation is not obvious and needs to be better understood in relation to digital societies. Last but not least, effective means to prevent manipulation are not easy to devise and can themselves have adverse effects. The goal of this panel is to discuss in a multidisciplinary way the issues raised by online manipulation, including the following questions:

- How can online manipulation be characterised and be distinguished from influence or nudging?
- How to draw a line between what can be accepted and what should be banned?
- When manipulation is based on the exploitation of human biases, how can it be identified and fought?
- What kind of legal and technical instruments could be used to effectively prevent or reduce the adverse effects of manipulation? What should be the role of the media in this context?

10:00 – Coffee Break

10:30 – ACCESS, MOVE AND PROTECT DATA IN THE AGE OF AI

Academic * Business * Policy *****

Organised by Intel

Chair Gwendal Le Grand, CNIL (FR)

Moderator Riccardo Masucci, Intel (BE)

Speakers Karolina Mojzesowicz, DG JUST (EU); Effy Vayena, ETH Zürich (CH); Michelle Richardson, Center for Democracy and Technology (US), B.N. Srikrishna, Supreme Court of India (retired) (IN)

Access to large and reliable datasets is essential to the development and deployment of artificial intelligence (AI). Improving access to data would be beneficial for making design more innovative, for better achieving public policy priorities and for increasing quality and quantity of services for citizens. The ability to process data and move it across borders allows for diversity and enhanced accuracy in datasets, and reduces the risks for unintended biases. Current data localization requirements around the world could hinder these opportunities. At the same time, AI technologies take advantage of ubiquitous data analytics and increased mechanisms for data collection and creation to make autonomous determinations in nearly real-time. In some cases, these decisions may affect individuals, their private lives, and their position in the society, leading to the need for public and private organizations to protect citizens and minimize adverse impacts.

- How the current situation could be improved by public-private initiatives aiming at promoting data access?
- Why policymakers should support the protected free flow of data and limit data localization requirements?
- How can automated decision-making be fostered while augmenting with safeguards to protect individuals?

11:45 – PROTECTING EU 2019 ELECTIONS - A JOINT RESPONSIBILITY

Business * Policy *****

Organised by Google

Chair Milan Zubiček, Google (BE)

Moderator Luukas Ilves, The Lisbon Council (BE)

Speakers Scott Carpenter, Jigsaw (US); Jens-Henrik Jeppesen, Center for Democracy & Technology (BE); Despina Spanou, DG CNECT (EU); Ulrik Trolle Smed, EPSC (EU)

Elections matter. Information matters. And during elections, access to accurate information is crucial. Digital attacks can take important websites offline, silencing information when voters need it most. Phishing attacks are very efficient and cheap ways to steal secret information from candidates. The panelists will discuss how can governments, public institutions and private sector work together to protect information against online attackers who aim at destabilizing democratic elections.

- How to improve cooperation between governments, public institutions and private sector while preventing online attacks during elections?
- What are the major online threats related to the EU 2019 elections and how to efficiently address them? How can we learn from past experiences?
- How to preserve trust in democratic elections in times of growing uncertainty? Are there some reasons for optimism?

13:00 – Lunch**14:15 – 14:20 CNIL-INRIA PRIVACY AWARD CEREMONY****Academic * Business * Policy ********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. Full description on page 13. The CNIL/INRIA Awardee(s) will present his/her/their paper at 16:00 in Area 42 Petit.

14:20 – BETWEEN TWO COMMISSIONS: GDPR – BRUSSELS EFFECT OR GLOBAL CONVERGENCE?**Academic * Business * Policy ********Organised by** IAPP**Moderator** Omer Tene, IAPP (US)**Speakers** Bruno Gencarelli, DG JUST (EU); Helen Dixon, Data Protection Commissioner (IE)

Eight months after its implementation date, GDPR is driving a sea change in data protection practices, including review of user interfaces, tightening of vendor agreements and appointment of thousands of data protection officers. More than just a European legal reform, GDPR has cross border effects from the U.S. to Brazil to Japan, including implications for foreign relations and trade policy. In this session, one of Europe's central data protection commissioners discusses first lessons from the GDPR rollout with the Head of the International Data Flows and Data Protection Unit at the European Commission. What is working and what isn't with GDPR? What are some of the unexpected implications of the legal reform?

- Is the new law fit for the socio-technological challenges ahead or is it obsolete out of the gate?
- How are new enforcement and compliance mechanisms, including one stop shop and the EDPB working in practice?
- How will policymakers react to disruptive changes, including Brexit and legal challenges to data transfer mechanisms?
- How does data protection interact with competition policy?

15:30 – Coffee Break**16:00 – DEFENDING THE GDPR: ONE YEAR ON****Academic ** Business ** Policy ******Organised by** CPDP**Chair** Věra Jourová, Commissioner: Justice, Consumers and Gender Equality (EU)**Moderator** Ruth Boardman, Bird & Bird (UK)

Speakers Stephan Micklitz, Google (DE); Michał Boni, MEP (EU); Marit Hansen, ULD (DE); Gloria González Fuster, VUB-LSTS (BE); Anna Fielder, EDRi (BE); Renate Nikolay, Cabinet of Commissioner Jourova (EU)

The GDPR has already applied for almost a year. In this time, there has been significant criticism of its substantive provisions and their practical impact on public bodies and businesses. Yet, this is the same Regulation that received generally positive responses across the board, these are the same substantive provisions that already appeared in the Directive and the same practical consequences already predicted in the legislative process. This panel considers this apparently contradictory situation and, in particular, considers the following questions:

- Where is all this criticism coming from?
- What form does it take?
- Is it justified?
- Where do we go from here?

17:15 – PRIVACY IMPACT ASSESSMENTS AND DEMOCRACY: SAFEGUARDING VOTER DATA**Academic *** Business * Policy ******Organised by** EPIC**Chair** Eleni Kyriakides, EPIC (US)**Moderator** Jennifer Daskal, American University Washington College of Law (US)

Speakers Romina Garrido, Fundación Datos Protegidos (CL); Amber Macintyre, Tactical Tech (DE); Marc Rotenberg, EPIC (US); Júlia Sziklay, Hungarian Data Protection Authority (HU)

Privacy impact assessments play a key role in safeguarding democratic institutions. In the US case EPIC v. Presidential Advisory Commission on Election Integrity, the efforts of the Trump voter commission to obtain personal voter data came to an end after EPIC argued that the Commission had failed to complete a privacy impact assessment required by law. In fact, just a few days after EPIC filed suit, the Commission suspended data collection and the personal data that had been wrongfully obtained was deleted. This panel explores the relationship between privacy (or data protection) impact assessments and the protection of democratic institutions in the United States and around the world. What lessons can be learned from EPIC v. Commission? And what are the strategies going forward to protect the privacy of voter data?

- How Privacy Impact Assessment can be a suitable safeguard even in the electoral field?
- Is Data Protection Impact Assessment from EU a model to be exported in the US?
- Electoral privacy should be regulated as a specific sector?

18:25 – EPIC INTERNATIONAL PRIVACY CHAMPION AWARD CEREMONY**Organised by** EPIC

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. Full description on page 13.

18:30 – Cocktail Sponsored by EPIC in Le Village

CPDP2019 PANELS AT AREA 42 GRAND

**8:45 – CONVERGING NORMS IN EMERGING MARKETS:
THE TRAJECTORY OF DATA PROTECTION REFORM IN ASIA****Academic * Business ** Policy *******Organised by** European Commission**Chair** Aaron Martin, TILT (NL)**Moderator** Ralf Sauer, DG JUST (EU)**Speakers** Clarisse Giroit, Asian Business Law Institute (SG); Hyunik Kim, Personal Information Protection Commission (KR); B.N. Srikrishna, Supreme Court of India (retired)(IN), Sinta Dewi Rosadi, University of Padjadjaran (ID)

This panel will bring together policy makers and experts from Asian countries such as India, Indonesia, Singapore and South Korea to discuss the region's experiences of reforming domestic legal frameworks in the light of global convergence towards a modern data protection system. Drawing also on the ongoing adequacy dialogue with the EU, the South Korean panelist will reflect on the importance of global convergence for cross-border data flows, while the Indian and Indonesian panelists will report on the national debates and policy-making process in drafting new data protection laws. The panel will also discuss how to combine convergence with national legal traditions and domestic institutional settings.

- What considerations have shaped data protection reform processes across Asian markets such as South Korea, Indonesia, and India?
- What are the economic drivers for data protection legal reform in the region?
- How have Asian countries balanced the interest in convergence with political or societal pressures to adopt data protection frameworks that reflect domestic realities?
- If convergence facilitates data flows, how do data localization rules fit into the picture?

10:00 – Coffee Break**10:30 – PRIVACY IN LATIN AMERICA: TOWARDS REGIONAL AND
GLOBAL CONVERGENCE****Academic * Business ** Policy *******Organised by** European Commission**Chair** Danilo Doneda, Brazilian Institute for Public Law (BR)**Moderator** Manuel García Sánchez DG JUST (EU)**Speakers** Argentinean Ambassador to the EU (AR); Laura Nahabetián Brunet, AGESIC (UY); Marcelo Drago, Consejo para la Transparencia (CL); Eduardo Bertoni, Agencia de Acceso a la Información Pública (AR); Isabela Ardalán, Atento (CO)

In addition to the achievements in terms of democracy consolidation and growth, Latin American countries have, over the years, showed a growing commitment to the protection of personal data. Argentina was the first Latin American country to be regarded as providing an

adequate level of protection for personal data transferred from the EU. In 2012, the European Commission adopted an adequacy decision concerning Uruguay that was also the first non-European country to join Convention 108. Since then, several countries in the region have adopted new data protection laws or started discussions towards the modernisation of existing ones. This momentum is also reflected in the adoption of the Ibero-American Data Protection Standards in 2017. These standards build on shared values and address common challenges, creating a stable framework to facilitate commercial flows and regulatory cooperation. This panel will bring together policy makers and experts from Latin-American countries such as Argentina, Brazil, Chile, Colombia and Uruguay to discuss the region's experiences of reforming data protection frameworks in the light of global convergence and regional integration. The speakers will report on these national and regional developments, including on the implementation of new laws. The panel will also discuss the benefits of global convergence and how to combine them with national legal traditions and domestic institutional settings.

- What have been the most important recent developments for privacy in Latin America? What about future perspectives?
- What are the expectations in terms of regional integration and global convergence on data protection?
- What should the next steps be to consolidate regional initiatives like the Ibero-American Data Protection Standards and the role of the Ibero-American Data Protection Network?

**11:45 – COPY/PASTE OR A FEEDBACK LOOP?
THE POST-GDPR DATA PROTECTION WORLD****Academic * Business ** Policy *******Organised by** BSA | The Software Alliance**Chair** Ana Brian Nougères, Estudio Jurídico BrianN y Asoc. (UR)**Moderator** Laura Linkomies, Privacy Laws and Business (UK)**Speakers** Aaron Cooper, BSA | The Software Alliance (US); Hiroshi Miyashita, Chuo University (JP); Michael Rose, US Department of Commerce (US); Bruno Gencarelli, DG JUST (EU); Laura Nahabetián Brunet, AGESIC (UR); Patricia Adusei-Poku, Ghana Data Protection Commission (GH)

The GDPR introduced robust requirements for data protection, security, and compliance when collecting and analyzing data tied to EU citizens - no matter where it is processed or stored. The regulation has sparked deliberations concerning data protection and privacy the world over, both on government and industry level. While there is no universal approach to privacy, the GDPR is a compass for future privacy rules and an important step forward for clarifying and protecting individual privacy rights. Countries around the world including the U.S., Brazil, India and Japan have entered or are now considering the next phases in their approaches to data privacy. This panel will bring together speakers from the EU and key jurisdictions to discuss how the world's data protection and privacy policy landscape is evolving post-GDPR and what lessons can be learned from the first months of GDPR's enforcement. Questions to be addressed include:

- How can the global data protection community balance the simultaneous global and regional pushes towards regulation?
- With more than 6 months of enforcement experience under its belt, what advice do EU

DATA PROTECTION AND DEMOCRACY

officials and stakeholders have to offer other regulators in the midst of drafting their own regulations?

- What questions do global stakeholders have for the EU?

13:00 – Lunch

14:15 – LEVERAGING ‘NUTRITION LABELS’ AND OTHER TOOLS FOR MORE RESPONSIBLE AI

Academic ** Business ** Policy **

Organised by Assembly (The Berkman Klein Center at Harvard University & MIT Media Lab)

Chair Kasia Chmielinski, Assembly (US)

Moderator Sarah Holland, Google (US)

Speakers Malte Beyer-Katzenberger, DG CNECT (EU); Clara Neppel, IEEE (AT); Jonnie Penn, University of Cambridge (UK); Ben Zevenbergen, Princeton University (US)

Algorithms make important decisions that affect our lives, from how we are policed to what advertisements we see online, and yet the datasets on which they're built are inconsistent, unrepresentative, and not always appropriately vetted for their use. The problem with bad outcomes isn't always the machine or the algorithm - it is often the health of the data itself. In an effort to address this problem, there are many initiatives around enabling 'healthier' datasets, borrowing from various standards paradigms. This panel will bring together experts across academia, standards bodies, and regulation to discuss methods for addressing problematic inputs.

- What information about a dataset should be available and accessible to a data scientist in order to support responsible model building?
- What information would be helpful for other audiences - policymakers, communities, etc - and how might this information differ depending on audience?
- What are some ways to present this information? Can we draw from parallel efforts in domains such as warning labels and nutrition labels?
- How might industry, government, and academia work together to create and support standards for dataset labeling?

15:30 – Coffee Break

16:00 – HOW THE ADEQUACY MECHANISM WORKS: PROGRESS IN THE EU'S GOVERNANCE OF CROSS-BORDER DATA FLOWS?

Academic ** Business * Policy ***

Organised by NEXA Center for Internet & Society

Chair Ugo Pagallo, NEXA Center for Internet & Society (IT)

Moderator Bojana Bellamy, Centre for Information Policy Leadership (UK)

Speakers Ralf Sauer, DG JUST (EU); Fumio Shimpō, Keio University (JP); Jos Dumortier, Timelex (BE); Kristina Irion, UvA (NL)

The GDPR's modernised 'adequacy' test in Art. 45 has sparked a hot debate among scholars and policy makers. The European Commission's communication from 2016 'Exchanging and Protecting Personal Data in a Globalised World' has shed some light into the procedure of adequacy assessments. It is still far from clear whether Art. 45 effectively guarantees the rights of individuals, or whether the mechanism can be interpreted in such a way, that it becomes more efficient. Whilst the European Commission has recognised Japan as having an adequate level of protection subject to several important restrictions, we may wonder whether the first application of the new catalogue of requirements in the GDPR's Art. 45 can represent a model for other countries. This panel promises a topical discussion in light of the pending Court of Justice's rulings and post-Brexit data flow arrangements.

- What are the implications of the adequacy finding in relation to Japan for other countries?
- Is the adequacy regime the bottleneck or the procedure?
- How can the EU adequacy mechanism become more efficient so as to protect individuals' rights and support the global flow of personal data?
- Given the turn-around, how can the Commission re-assess all existing adequacy findings in the four years after the GDPR enters into force?

17:15 – GLOBAL LEGAL FRAGMENTATION AND INTEROPERABILITY

Academic * Business ** Policy ***

Organised by US Department of Commerce

Chair Carol Evrard, Stibbe (BE)

Moderator Hilary Wandall, TrustArc (US)

Speakers Michael Rose, US Department of Commerce (US); Amba Kak, Mozilla (IN); Ana Brian Nougères, Estudio Jurídico BrianN y Asoc. (UR); Mac Yokozawa, Kyoto University (JP), Alisa Vekeman, DG JUST (EU)

This panel will explore the increasing threat of global legal fragmentation in privacy legislation. In the last four years, the OECD has updated its Privacy Guidelines, APEC has updated its Privacy Framework, and the GDPR began regulating privacy throughout the EU. However, as countries around the world seek to regulate privacy in an ever more digital world, legal fragmentation between privacy protections risks stifling innovation, hurting economic development, and creating dramatically different privacy protections for consumers depending on physical location. The panel will discuss this trend and seek to address how interoperability of privacy laws through existing mechanisms such as adequacy findings or certification mechanisms can bridge this divide.

- What are the trends in privacy laws which are most concerning to you from the perspective that they will create fragmented protections for consumers?
- What existing mechanisms can bridge the challenge of this trend towards fragmentation?
- If we accept the premise that all laws won't look the same, how do you ensure privacy protections travel with the data regardless of where it is transferred?
- One commonality of many recently passed privacy laws and international agreements is the idea of company-based certifications. How can this be implemented globally to solve the challenges fragmentation creates?

18:30 - Cocktail Sponsored by EPIC in Le Village

DATA PROTECTION AND DEMOCRACY

8:45 – REGULATING ARTIFICIAL INTELLIGENCE - IS THE GDPR ENOUGH?

Organised by CPDP

Chair Ian Brown, Research ICT Africa (UK)

Speakers Paul Nemitz, DG JUST (EU); Mireille Hildebrandt, VUB-LSTS (BE); Ben Zevenbergen, Princeton University (US)

The development of Artificial Intelligence/Machine Learning tools often depends on vast quantities of data - frequently personal data as defined by the GDPR. Given the extensive limits and controls applied by the GDPR (and the fundamental rights to privacy and data protection underpinning it in EU law), will the developing interpretation of these laws by national courts and the Court of Justice fully protect EU residents' rights - or will further ex ante regulation be required? In this Oxford Union-style debate, three leading experts will speak for 10 minutes each for and against the motion that "This House believes the GDPR will not be enough to regulate Artificial Intelligence". They will then debate the motion with the audience, before a final vote is held. Join us for what we hope will be one of the liveliest and least consensual sessions at CPDP!

10:00 – Coffee Break

10:30 – BLOCKCHAIN TECHNOLOGY AND THE GDPR: THE BEGINNING OF A BEAUTIFUL PRIVACY WHAC-A-MOLE?

Academic * Business * Policy ****

Organised by Blockchain and Society Policy Research Lab, Institute for Information Law, UvA

Chair Balazs Bodo, Blockchain and Society Policy Research Lab, Institute for Information Law, UvA (NL)

Moderator Mireille Hildebrandt, VUB-LSTS (BE)

Speakers Michèle Finck, Max Planck Institute for Innovation and Competition (DE); David Ciliberti, DG JUST (EU); Alexandra Giannopoulou, Blockchain and Society Policy Research Lab, Institute for Information Law, UvA (NL); George Danezis, UCL (UK); Konstantinos Stylianou, University of Leeds (UK)

Individual user control of data has become a central issue in the European Data Protection Regulation (GDPR), creating a more demanding data protection framework for involved actors, all while coming in conflict with fundamental characteristics of blockchains. Thus, the difficulty lies in designing a system without compromising core values of both privacy regulation on the one hand and blockchain technology on the other. Given the right incentives there is no doubt GDPR compliant distributed ledgers can, and will be designed. The real question is what happens if there is persistent market/social/political interest in those blockchain implementations which do not care for, or are unable to achieve GDPR compliance. Considering the interdisciplinary nature of the main question, the proposed panel consists of invited experts selected to cover various

privacy-related fields including law and computer science.

- What are the main points of friction between blockchains and the GDPR?
- What are the technological privacy enhancing mechanisms that could apply?
- What are the appropriate and necessary conciliations for the creation of privacy-preserving blockchains in accordance with data protection regulation?
- Is there a market for non-compliance that blockchain technologies are best suited to serve?

11:45 – AI GOVERNANCE: ROLE OF LEGISLATORS, TECH COMPANIES AND STANDARDS BODIES

Academic * Business ** Policy ***

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

Chair Mark Cole, University of Luxembourg (LU)

Moderator Erik Valgaeren, Stibbe (BE)

Speakers Alain Herrmann, National Commission for Data Protection (LU); Christian Wagner, University of Nottingham (UK); Jan Schallaböck, iRights/ISO (DE); Janna Lingenfelder, IBM/ISO (DE)

AI calls for a "coordinated action plan" as recently stated by the European Commission. With its societal and ethical implications, it is a matter of general impact across sectors, going beyond security and trustworthiness or the creation of a regulatory framework. Hence this panel intends to address the topic of AI governance, whether such governance is needed and if so, how to ensure its consistency. It will also discuss whether existing structures and bodies are adequate to deal with such governance, or, if we perhaps need to think about creating new structures and mandate them with this task. Where do we stand and where are we heading in terms of how we are collectively dealing with the soon to be almost ubiquitous phenomenon of AI?

- Do we need AI governance? If so, who should be in charge of it?
- Is there a need to ensure consistency of such governance?
- What are the risks? Do we know them and are we in the right position to address them?
- Are existing structures/bodies sufficient to address these issues or do we perhaps need to create new ones?

13:00 – THE CLOUD ACT AND E-EVIDENCE: "AMERICA FIRST" OR GDPR FIRST? CHALLENGES OF TRANSATLANTIC ACCESS TO E-EVIDENCE IN LAW ENFORCEMENT

Organised by Privacy Platform

Moderator Sophie in 't Veld, MEP (EU)

Speakers Katitza Rodriguez, EFF (US); Guido Brinkel, Microsoft (DE); Jennifer Daskal, American University Washington College of Law (US); Mark Gray, DG JUST (EU)

In March last year the US CLOUD Act was passed as part of a two-thousand page spending bill covering 1.3 trillion dollars, without any congressional debate. A few months later, the European Commission published its e-evidence regulation proposal for easier access to electronic evidence

for law enforcement purposes. By the end of January, the Commission will recommend the Council to grant a mandate for negotiations with the US on an EU-US agreement under the CLOUD Act. What are the consequences of the CLOUD Act and a forthcoming EU-US agreement for data privacy of Europeans? Are the US and EU racing against each other to the bottom: weaker privacy protections and eliminating judicial checks and legal safeguards? Will the EU propose the same arrangement to Russia or China if they adopt their own CLOUD Act? How can law enforcement cooperation work in the digital age without compromising citizens' rights?

14:15 – MICRO-TARGETING, COMPUTATIONAL PROPAGANDA, PRIVACY, AND DEMOCRACY

Academic ** Business ** Policy **

Organised by Fraunhofer Institute for Systems and Innovation Research ISI, Forum Privacy

Chair Elias Kyewski, University of Duisburg-Essen (DE)

Moderator Nicholas Martin, Fraunhofer ISI (DE)

Speakers Frederik Zuiderveen Borgesius, Radboud University Nijmegen (NL); Vidya Narayanan, Oxford Internet Institute (UK); Sanne Kruijkemeier, UvA (NL); Olivier Micol, DG JUST (EU); Aikaterini Poulou, EDPS (EU)

Political actors are deploying ever-more fine-grained forms of data and social media-based messaging to persuade voters, mobilise supporters, disrupt opponents and shape public discourse. Two sets of practices have received particular attention; micro-targeting (serving targeted messages based on detailed personal profiling) and computational propaganda focused on manipulating discourse (fake news, bots, etc.). We still struggle how to evaluate and respond to these new political technologies. They raise privacy concerns, threaten to exacerbate polarisation and crises of trust, and have been held responsible for political violence. Regulatory responses pose their own dilemmas, both with respect to protecting privacy and free speech. Moreover, these technologies' impacts may not be exclusively negative, but also help reinvigorate democratic participation. The panel will debate the nature, effects, privacy risks and possible regulation from the perspectives of law, communication studies and psychology, social science and regulatory practice.

- How do micro-targeting and computational propaganda relate to each other?
- What effects do they have on citizens, publics and the democratic process?
- What risks to privacy and data protection do these practices pose?
- What rules and regulatory responses do we need?

15:30 – Coffee Break

16:00 – DATA IS (POLITICAL) POWER!

Organised by University of Amsterdam (IViR & ASCoR)

Chair Natali Helberger, UvA (NL)

Moderator Tom Dobber, UvA (NL)

Speakers Daniel Kreiss, University of North Carolina at Chapel Hill (US), Stefania Milan, UvA (NL), Julia Reda, MEP (EU), Jennifer Childs, ICO (UK)

When discussing political microtargeting, we often talk about the persuasiveness of the technique, its manipulative nature, and the consequences of the use of such a potentially persuasive force for our democratic society (e.g., Gorton, 2016; Zuiderveen Borgesius et al., 2018). Social platforms play an important role, facilitating microtargeting, by offering the infrastructure for potentially effective persuasion. Apart from these very relevant issues, there is another important issue that follows from the digital intermediaries' wealth in terms of personal data and their elaborate persuasion infrastructure: the digital intermediaries' own political power. For example, how do data make digital intermediaries, such as Facebook, a political player? And how powerful are these players, politically? Social platforms increasingly do more than just facilitating political communication. For example, by lobbying, donating to specific politicians, and by offering advice to political campaigns, social platforms actively interfere in the public debate. As such, these platforms are turning into political actors themselves. The goal of this panel is three-fold:

- to understand the concept and implications of social platforms like Facebook, YouTube or Twitter for, and as political players, with a particular focus on the upcoming EU elections,
- to examine if, and why, from a democratic point of view, the political power of social platforms is problematic,
- to explore the role of law and policy makers in providing the necessary checks-and-balances of that political power.

17:15 – MISSION IMPOSSIBLE: DATA PROTECTION IN AT-RISK ORGANISATIONS

Academic * Business ** Policy ***

Organised by École Polytechnique Fédérale de Lausanne (EPFL)

Chair Alessandra Pierucci, Italian Data Protection Authority (IT)

Moderator Stevens Le Blond, Neutrality (CH), formerly EPFL (CH)

Speakers Harlo Holmes, Freedom of the Press Foundation (US); Gus Hosein, Privacy International (UK); Marek Marczykowski-Górecki, Qubes OS and Invisible Things Lab (PL); Massimo Marelli, International Committee of the Red Cross (INT)

From state-sponsored cyber attacks to mass surveillance, effective data security in organizations operating in adverse environments is nearly impossible today. This panel will discuss the extreme legal, technological and organizational challenges that these organizations must overcome to carry out their work. We will discuss the trade-offs between operational security and practical requirements, and the need to complement legal protection with robust technological safeguards.

- At-risk organizations must protect data of vulnerable users, despite susceptibility to coercion, etc. What are the unique needs of organizations operating in armed conflicts and other situations of violence?
- Technology is a key component of data protection but usability often decreases with security. How to tailor such technology to legal and organizational factors of at-risk organizations?
- Societal improvements do not occur in a vacuum. How can at-risk organizations leverage third-parties without hampering data protection?

18:30 – Cocktail Sponsored by EPIC in Le Village

DATA PROTECTION AND DEMOCRACY

8:45 – ACCESSING YOUR PERSONAL DATA: REAL EMPOWERMENT OF THE DATA SUBJECT?

Organised by Nymity

Chair Martin Abrams, Information Accountability Foundation (US)

Moderator Gabriela Zafir-Fortuna, Future of Privacy Forum (US)

Speakers Paul Breitbarth, Nymity (NL); Laura Drechsler, VUB-LSTS (BE); Emerald de Leeuw, Eurocomply (IE); Simon Hania, Uber (NL)

Since the introduction of GDPR in 2018, more people are aware that data protection exists, and that they have rights to better understand what is happening with their data. One of the pillars of the data protection reform was to improve the power of data subjects, including by extending their rights. Privacy statements need to be clearer and organisations are bound to stricter deadlines to respond. Also in other jurisdictions, including California and Brazil, legislation was passed to underline the importance of data subject rights, and especially the right of access. But has the empowerment of the data subject so far succeeded? This panel will discuss the implementation of the right of access so far, as well as what could be done to ensure the right of access can be a real success for individuals and companies around the world.

- What does the right of access look like from a global perspective?
- Has it really become easier for data subjects to request access to their data?
- Are companies able to meet their deadlines, and how do they ensure they can provide the relevant data?
- What best practices exist to improve the right of access?

10:00 – Coffee Break

10:30 – SHAPING TECHNOLOGY AROUND GDPR REQUIREMENTS

Academic * Business ** Policy ***

Organised by European Union Agency for Network and Information Security

Chair Athena Bourka, ENISA (EU)

Moderator Marit Hansen, ULD (DE)

Speakers Jason Novac, Apple (US); Gro Mette Moen, Norwegian Consumer Council (NO); Cedric Lauradoux, Inria (FR); Alessandro Mantelero, Politecnico di Torino (IT); Achim Klabunde, EDPS (EU)

In the aftermath of large-scale data breaches and illegal processing of personal data, it has become apparent that data protection legal obligations need to be backed-up by robust technological protection measures. The principles of data protection by design and default, as enshrined in GDPR, can broadly support this approach, however the practical implementation of these principles is far from advanced. Software developers lack best practice examples, while data controllers struggle to select the appropriate solutions for their processing operations in a

market flooding with software of disputable quality. In the light of new technological challenges, such as advanced tracking techniques and autonomous agents, the aim of the panel is to discuss how technology can be shaped around GDPR requirements and focus on specific best (and bad) practices in the field.

- What is the notion of 'by design' and how can technologies be 'shaped' to support data protection?
- Which technologies can help implement data minimisation and transparency?
- What is the role of pseudonymisation as a privacy by design technique?
- What is the role of the default settings?
- What are the broader challenges of defining data-driven solutions that support human rights and ethics?

11:45 – TRANSPARENCY BY LEGAL DESIGN

Academic * Business ** Policy ***

Organised by Université Catholique de Louvain, UCLouvain

Chair Sari Depreeuw, Université Saint-Louis - Bruxelles (BE)

Moderator Rossana Ducato, UCLouvain (BE)

Speakers Fenneke Buskermolen, DG CNECT (EU); Antti Innanen, Dottir Attorneys (FI); Tom Norton, Fordham University (US); Monica Palmirani, Università di Bologna (IT); Arianna Rossi, University of Luxembourg (LU); Christoph Schmon, BEUC (BE)

The GDPR has expressly codified transparency as a fundamental data protection principle. In particular, the Regulation requires that information notices, communications to the data subjects and requests for consent must be drafted "in a concise, transparent, intelligible and easily accessible form, using clear and plain language", highlighting the importance of taking the target audience into consideration (e.g. in case the information is addressed to children). Along the same line, the proposed ePrivacy Regulation moves towards new transparency obligations. But how can such a principle be implemented in practice? Legal Design is an innovative approach that can shed some lights on this challenge. It is an interdisciplinary field that combines design methodology, insights from behavioural law and economics, and IT to pursue a legal goal. The aim of the panel is to present the foundations of Legal Design and show some of its practical applications in the field of data protection.

- What is Legal Design?
- Can Legal Design pursue the GDPR policy goal of providing data subjects with meaningful information?
- How can visualisation and icons foster data subjects' understanding of their rights?
- What lessons can we learn from Legal Design to pave the way for the implementation of the transparency requirement in relation to AI tools?

13:00 – Lunch

14:15 – UNCOVERING THE HIDDEN DATA ECOSYSTEM

Academic ** Business ** Policy **

Organised by Privacy International

Chair Ailidh Callander, Privacy International (UK)

Moderator Aliya Ram, Financial Times (UK)

Speakers Johnny Ryan, Brave Browser (US); Paul-Olivier Dehaye, Personal Data IO (CH); Joana Moll, Critical Interface Politics - HANGAR (ES); Katarzyna Szymielewicz, Panoptikon Foundation (PL)

In November 2018, complaints were filed against seven data brokers, ad-tech companies and credit referencing agencies with data protection authorities in France, Ireland, and the UK. These complaints target companies that, despite exploiting the data of millions of people, are not household names and therefore rarely have their practices challenged. It's incredibly difficult - even for experts - to understand what is happening to our data. Nowhere is such data exploitation more persistent and systemic than in the complex data ecosystem. The drive to create targeted ads has created an entire ecosystem made up of thousands of companies in the business of tracking and profiling people in virtually all aspects. Uncovering the ecosystem is hard and holding the system to account even harder. The panel will shed light on the ecosystem, raise questions around the impact of GDPR on the ecosystem, and discuss lessons learned from academics, civil society, regulators, journalists, and industry.

- Why is the data ecosystem so complex and often hidden?
- Has GDPR changed anything?
- What regulatory enforcement action are we going to see in 2019?
- How can individuals, civil society, journalists and artists shed light into the hidden data ecosystem?

15:30 – Coffee Break

16:00 – IMPLEMENTING PRIVACY BY DESIGN INTO MOBILE DEVELOPMENT, OBSTACLES AND OPPORTUNITIES. A DEVELOPER PERSPECTIVE ON DATA PROTECTION BY DESIGN

Academic * Business * Policy ****

Organised by AppPETs Project

Chair Daniel Guagnin, Praemandatum (DE)

Moderator Seda Gürses, KU Leuven (BE)

Speakers Wulf Bolte, mediaTest digital (DE); Martin Lopatka, Mozilla (NL); Veronica Buer, Datatilsynet (NO); Vesa-Matti Hartikainen, Jolla (FI)

The GDPR is now in place and brings new obligations for data protection and privacy enhancing technologies. But do we now see technologies designed to empower individuals and to regain control over their digital shadows? Together with developers of PETs, entrepreneurs who are selling privacy enhancing products, and policy practitioners, we want to discuss how we can practically advance the adoption of privacy by design into mobile development. For that

we want to put a focus on the developers' perspective - who in the end have to implement the code. We want to talk about the current challenges and obstacles in deploying PETs and possible solutions and approaches, from best practice guidelines to privacy enhancing libraries.

- Does the GDPR's demand of technical solutions for data protection by design lead to the deployment of PETs?
- What else is necessary to finally get these solutions into broad deployment?
- What are the obstacles for developers and deployers?
- How can we generate consumer demand for PET?

17:15 – CERTIFICATION FOR GDPR-COMPLIANT ANONYMITY: REAL ANONYMISATION OR JUST ANOTHER RISK ASSESSMENT?

Academic * Business ** Policy ***

Organised by Aircloak

Chair Max von Grafenstein, University of the Arts Berlin (DE)

Moderator Felix Bauer, Aircloak (DE)

Speakers Paul Francis, Max Planck Institute for Software Systems (MPI-SWS) (DE); Lorraine Maisnier-Boché, McDermott, Will & Emery (FR); Félicien Vallet, CNIL (FR); Ilya Vasilenko, Teralytics (CH)

An important aspect of data protection is data anonymity---allowing statistical knowledge to be obtained from data while protecting individual data. GDPR considers anonymised data to no longer be personal data, and as such does not need to be protected. GDPR also expects national bodies to establish certification programs, including for anonymisation. It is, however, very difficult to know when data is adequately anonymised, and therefore difficult to establish certification programs for anonymity. This panel explores the problems and initial steps towards anonymisation certification. The panel includes data owners, data controllers, Data Protection Authorities (DPA), anonymisation technologists, and privacy legal scholars. From these various and differing perspectives, the panel will describe the state of DPA certification programs, and explore the extent to which anonymisation can truly be determined, methods for doing so, and the role that risk assessment plays.

- What are the GDPR requirements for certification programs for anonymisation?
- What is the status of anonymisation certification programs?
- What are the technical and legal challenges for anonymisation certification?
- What role does risk assessment play in anonymisation certification?

18:30 - Cocktail Sponsored by EPIC in Le Village

8:45 – COMPETITION, PRIVACY & SOCIETY IN THE DIGITAL ERA

Academic ** Business ** Policy **

Organised by Transatlantic Consumer Dialogue (TACD) and BEUC

Chair Tomaso Falchetta, Privacy International (UK)

Moderator Anna Fielder, TADC (UK)

Speakers Agustin Reyna, BEUC (BE); Orla Lynskey, LSE (UK); Liza Lovdahl Gormsen, BIICL (UK); Alexandros Papanikolaou, DG COMP (EU)

Society and consumer welfare require the existence of competitive markets driven by choice and innovation, so individuals can choose freely among a wide range of contents, services and products. However, in recent years digital platforms have concentrated and wielded enormous powers, due to the processing of vast amounts of personal data. Their powers can cause privacy and economic harms, such as degradation of service or exclusion from information. Increased exploitation of this data, combined with micro-targeting by corporations, has also resulted in practices which have bad implications for the working of democratic institutions. Further, it is argued that GDPR may have negative impacts on competition, as new entrants do not have the access to the data possessed by corporations. As a result of these trends there is now big focus on how to apply traditional competition law in digital markets.

- Do complex technologies and sophisticated abuses of market power call for adjustments to the goals and scope of competition law enforcement?
- How should authorities re-interpret competition regulations to address privacy and other challenges by massive data exploitation?
- What does “consumer welfare” mean in digital markets regarding zero-price services?
- How can privacy, competition and consumer protection law cooperate and complement each other?

10:00 – Coffee Break

10:30 – SMART CITY GOVERNANCE: CITIZENS, PRIVACY AND SERVICES

Academic * Business * Policy ****

Organised by Centre for Research into Information, Surveillance and Privacy

Chair Valentina Pavel, Privacy International (UK)

Moderator Ola Svenonius, Swedish Defense Research Agency (SE)

Speakers David Murakami Wood, Queens University (CA); Mirko Schaefer, Utrecht University (NL); Sara Degli-Esposti, Consejo Superior de Investigaciones Científicas (ES); William Webster, University of Stirling CRISP (UK); Max von Grafenstein, University of the Arts Berlin (DE)

Smart City (SC) developments are embedding digital technologies in all aspects of urban life. Typically, the focus is more efficient services and better-informed policy-making. The SC umbrella covers a range of technologies/practices, including sensory devices, large data sets, data science,

sentiment analysis, new apps and dashboards (etc.). Whilst the focus has been on service delivery there is an increasing awareness that these technologies can be used for citizen engagement and novel governance practices - to empower service users and citizens. There has also been an increasing awareness of the data intensity of these SC practices and concern about the privacy/data protection implications, with commentators referring to SC's as 'Smart Surveillance Cities', primarily because the possibilities offered rely on the collection, processing and matching of vast quantities of personal data. Drawing on academic, activist, practitioner and regulatory perspectives, this panel examines the privacy issues in a contemporary SC environment.

- What are the privacy and data protection issues relating to Smart City
- How is privacy and data protection managed in the Smart City context?
- To what extent are citizens and service users engaged in the governance of privacy in Smart Cities?
- Are Smart Cities by definition also Smart Surveillance Cities?

11:45 – VALUES AND ETHICS IN INNOVATION FOR RESPONSIBLE TECHNOLOGY IN EUROPE

Academic ** Business ** Policy **

Organised by Politecnico di Torino

Chair Eleni Kosta, Tilburg University (NL)

Moderator Alessandro Mantelero, Politecnico di Torino (IT)

Speakers Irina Shklovski, IT University of Copenhagen (DK); Christian D'Cunha, EDPS (EU); Javier Ruiz Diaz, Open Rights Group (UK); Alison Powell, LSE (UK); Annelie Berner, Copenhagen Institute of Interaction Design (DK)

Data-intensive products and services raise questions about the values embedded in them. These values shape how information is processed to profile and classify individuals and groups to take decisions that concern them or may affect their behaviour. Data protection then becomes a constituent element of citizenship. Digital democracy cannot operate with data-enabled social stigma and behaviour control. There is a risk that “algorithmic truth” prevails over democratic decisions. Collective issues concerning ethical and social impact of data use must therefore be adequately addressed in developing data governance models in the early design stage of products and services. Societal consequences should be assessed using open and participatory solutions. Engaging with products and services at the point of design allows us to reach beyond privacy laws to embed ethical considerations that cultivate moral values and capabilities in practice without undermining necessary regulations.

- How can data protection and GDPR properly address the societal consequences of data use?
- How do developers of IoT projects and services enact practices with ethical significance and consequence?
- How can considerations of ethics be translated into practical policy and design recommendations?
- How can design for speculation encourage the consideration and imagination of broader socio / economic / political / ecological implications of the new technology we make?

13:00 – Lunch**14:15 – JUNIOR ACADEMIC SESSION 1****Academic *********Organised by** CPDP**Chair** Ignacio Sanchez, JRC (EU)

Authors Geert Lokhorst, UvA (NL) and Mireille van Eechoud, UvA (NL); Gianclaudio Malgieri, VUB-LSTS (BE); Domenico Rosani, University of Innsbruck (AT); Mara Paun, Tilburg University (NL)

- Malgieri - Right to Explanation and Algorithm Legibility in the EU Member States Legislations - Suitable Safeguards for automated decision-making within national implementations of the GDPR
- Lockhorst - Jacks of All Trades – Public Registers, Personal data & Principles of Proportionality
- Rosani - Child's participation online and the General Data Protection Regulation – a dialogue between educational and legal sciences is urgently needed
- Paun - Consumer Protection in Financial Services: Source of inspiration for data protection?

15:30 – Coffee Break**16:00 – JUNIOR ACADEMIC SESSION 2****Academic *********Organised by** CPDP**Chair** Jef Ausloos, IVIR (NL)

Authors Yordanka Ivanova, Sofia University "St. Kliment Ohridski" (BG), Svetlana Yakovleva, UvA (NL), Wanshu Cong, McGill University (CA), CNIL/INRIA Privacy Award Winner(s)

- Ivanova - Privacy and Freedom of Expression to Counter Fake News and Other Threats to Democracy
- Yakovleva - Privacy Protection(ism)
- Cong - Privacy and Data Protection: Solving or Reproducing the Democratic Crisis of the Neo-liberal Capitalism?
- CNIL/INRIA Privacy Award Winner(s)

17:15 – SENIOR ACADEMIC SESSION 1**Academic *********Organised by** CPDP**Chair** Eduard Fosch-Villaronga, Leiden University (NL)

Authors Michael Birnhack, Tel Aviv University (IL) and Tal Morse, Hadassah College (IL); Michele Loi, University of Zurich (CH) and Markus Christen, University of Zurich (CH); Wolfgang Schulz, Hans-Bredow-Institut for Media Research (DE), Florian Wittner, Hans-Bredow-Institut for Media Research (DE), Kai Bavendiek, Hamburg University of Technology, Institute for

Software Systems (DE) and Sibylle Schupp, Hamburg University of Technology, Institute for Software Systems (DE)

- Birnhack and Morse - The Posthumous Privacy Paradox: Users' privacy preferences and behavior regarding digital remains
- Loi and Christen - Two concepts of group privacy
- Schultz et al. - Modeling and verification in GDPR's Data Protection Impact Assessment

18:30 - Cocktail Sponsored by EPIC in Le Village

RE-CODING BLACK MIRROR WORKSHOP@CPDP2019 AT MAISON DES ARTS

08.30 - Welcome and Introduction by Paul De Hert in Grande Halle**8:45 – 9:50 SESSION 1 : PRESENTATIONS (15 MINS PRES. + 5 MINS QUESTIONS)**

- "It's not real, but it helps" – Societal and ethical challenges of robotic care technologies, Roger Søråa.
- "Am I talking to a bot or a human?" - Transparency in pseudo-AI systems, Claudine Bonneau and Régis Barondeau
- Transparency and performance in dystopian social media environments - Joana Bárbara Fonseca

09:50 - 10:30 Coffee Break**10:30 - 11:45 SESSION 2 : PRESENTATIONS (15 MINS PRES. + 5 MINS QUESTIONS)**

- Privacy, Security and Trust in the Internet of Neurons – Diego Sempreboni and Luca Viganò
- When Thoughts Betray You: Neural Security and the World of "Black Mirror" – Katherine Pratt
- "Smart Humans... WannaDie?" – Diego Sempreboni and Luca Viganò

11:45 - 12:00 Coffee Break**12:00 - 12:45 SESSION 3 : PRESENTATIONS (15 MINS PRES. + 5 MINS QUESTIONS)**

- Privacy, Security and Trust in the Internet of Neurons – Diego Sempreboni and Luca Viganò
- When Thoughts Betray You: Neural Security and the World of "Black Mirror" – Katherine Pratt
- "Smart Humans... WannaDie?" – Diego Sempreboni and Luca Viganò

DATA PROTECTION AND DEMOCRACY

12:45 - 14:15 Lunch**14:15 - 14:45 HANDS-ON SESSION I**

- Schroedinger's Man, Diego Sempredoni and Luca Viganò
- Instructions and team-up

14:45 - 16:30 HANDS-ON SESSION II

- Prepare your dystopic sci-fi scenarios

16:30 - 18:00 LAST SESSION

- Scripts Presentation
- Debate on technological future
- Discussion, final remarks and feedbacks

18:30 - Cocktail Sponsored by EPIC in Le Village

THURSDAY 31st JANUARY 2019

CPDP2019 PANELS AT GRANDE HALLE

8:45 - DATA QUALITY: AN OFTEN OVERLOOKED ASPECT IN FUNDAMENTAL RIGHTS COMPLIANT DATA PROCESSING**Academic ** Business ** Policy ******Organised by** EU Agency for Fundamental Rights**Chair** Diana Dimitrova, FIZ Karlsruhe (DE)**Moderator** Elise Lassus, FRA (EU)**Speakers** Athena Bourka, ENISA (EU); David Reichel, FRA (EU); Pat Walshe, Privacy Matters (UK); Daniel Drewer, Europol (EU)

Recent developments have led to an enormous increase in the use of data, including the use of data for building machine learning and predictive models to support decisions. New technologies also come with potential challenges to fundamental rights, such as the right to privacy and data protection or non-discrimination. To mitigate potential challenges, an assessment of data quality is one important measure. There is, however, the need for clear guidance on how to assess and ensure data quality for processing data for different purposes. In this panel, the challenge of effectively assessing and maintaining the quality of data for data protection and fundamental rights compliant processing will be discussed.

- What does quality of data mean for data protection and AI systems?
- How can the data be effectively assessed? What are the sources of error?
- How does low quality of data impact on fundamental Rights?

10:00 - Coffee Break**10:30 - FROM RESEARCH TO PRODUCT LAUNCH: MULTISTAKEHOLDER PERSPECTIVES ON AN ETHICAL AND PRIVACY-BY-DESIGN APPROACH TO ARTIFICIAL INTELLIGENCE****Academic ** Business ** Policy ******Organised by** Facebook**Chair** Jens-Henrik Jeppesen, Centre for Democracy and Technology (BE)**Moderator** Norberto Andrade, Facebook (EU)**Speakers** Christoph Lütge, Technische Universität München (DE); Andrea Renda, CEPS (BE); Frederike Kaltheuner, Privacy International (UK); Pierre-Emmanuel Mazaré, Facebook (FR)

Artificial Intelligence is a fast-growing technology that already has a significant impact on our day-to-day lives. As with any technology, AI raises a number of ethical and legal questions, in particular around fairness and accountability in automated decision-making. Data protection and privacy considerations are an essential aspect of AI, and the GDPR already addresses some of these challenges as part of its provisions on automated decision-making. The purpose of this panel is to understand and discuss how companies are building - and should be building - AI into their services with privacy and ethics in mind. The panel will discuss the risks and opportunities that AI poses from the perspectives of regulators, academia and civil society. We will then take a deep dive into how Facebook is developing AI-based processes and tools with a privacy- and ethics-by-design approach, and how we are advancing the state-of-the-art in AI through open research and academic collaborations.

- What are the most salient risks and opportunities around AI that policymakers and regulators should take into account?
- What ethical and privacy considerations should companies should take into account as they build AI systems?
- How should we resolve some of the tensions that arise from AI systems making decisions in areas where even humans don't always agree on the right outcome?
- What are the most effective ways for stakeholders to build collaborative, evidence-based policy proposals around AI?

11:45 - LAW ENFORCEMENT AND DATA SUBJECTS' RIGHTS: IS THE EU LEGAL FRAMEWORK A GENUINE STEP FORWARD?**Academic *** Policy *******Organised by** CPDP**Chair** Daniel Drewer, Europol (EU)**Moderator** Clara Guerra, Portuguese DPA (PT)**Speakers** Gert Vermeulen, Belgian Data Protection Authority (BE); Vagelis Papakonstantinou,**DATA PROTECTION AND DEMOCRACY****COMPUTERS, PRIVACY & DATA PROTECTION**

VUB-LSTS (BE); Hielke Hijmans, Centre for Information Policy Leadership (BE);
Anna Moscibroda, DG JUST (EU)

Directive 2016/680 creates a harmonized data protection framework for Member State law enforcement authorities, excluding the national security authorities and Europol. Amongst the highlights of this framework is the strengthened level of protection of data subjects' rights, e.g. of access, rectification, erasure and restriction of processing. The strengthened rights are expected to grant more transparency to the data subjects and act as safeguards against the law enforcement authorities. However, the legal framework contains many exceptions. In addition, subjects' rights were already provided for in existing EU law enforcement instruments such as the Schengen Information System, which are not necessarily harmonized with Directive 2016/680. At the same time, the limited scope of Directive 2016/680 – which excludes the national security authorities and EU entities such as Europol (which is subject to a separate legal framework) – begs the question of how effectively Directive 2016/680 will boost data subjects' rights. Core questions:

- Have the Member States modified the existing procedures for exercise of the rights, esp. those Member States which provided only for indirect exercise of the rights through the responsible DPA? What are the trends?
- Has Directive 2016/680 led to increases in the number of data subjects' requests to exercise their rights? Why (not)?
- Has cooperation on EU level between national supervisory authorities and these and Europol and the EDPS improved?
- Do Directive 2016/680 and the implementing national laws contain loopholes which allow for too broad exceptions/restrictions, e.g. restricting the right of access on national security or other grounds?

13:00 – Lunch

14:15 – FACIAL RECOGNITION SYSTEMS - FROM FALSE POSITIVES TO POSITIVELY FRIGHTENING

Academic ** Business * Policy ***

Organised by CPDP

Chair Rosamunde van Brakel, VUB-LSTS (BE)

Moderator Ben Hayes, Transnational Institute/DPSM Ltd. (UK)

Speakers Megan Goulding, Liberty (UK); Jay Stanley, ACLU (US); Karolina Mojzesowicz, DG JUST (EU); Pedro Torres, Vision Box (PT); Sandra Leaton Gray, Biometrics Institute (UK)

Once seen as something of a benign biometric, digitised photographs and facial recognition systems are everywhere. From Apple's move from TouchID to FaceID, UK police forces' rollout, Taylor Swift's anti-stalker deployment, Amazon's tech falsely matching mugshots to members of Congress, China's wholesale embrace, Microsoft waking-up to the face surveillance society and suspicions that the #10YearChallenge is a ruse for machine learning, facial recognition is big news. Once the stuff of fantasy, serious resources are now invested in the development of a new generation of systems capable of detecting emotion, intentions and "suspicious behaviour".

- What are the latest technological developments in facial recognition?
- What are the legal, social and ethical issues raised?
- What ethical and scientific issues are raised by R&D projects?
- What are potential regulatory responses?

15:30 – Coffee Break

16:00 – AVOIDING A RACE TO THE BOTTOM IN CROSS-BORDER ACCESS TO DATA

Academic * Business ** Policy ***

Organised by EDRI and EFF

Chair Thomas Boué, BSA | The Software Alliance (BE)

Moderator Diego Naranjo, EDRI (BE)

Speakers Peter Kimpian, Council of Europe (INT); Maximilian Schubert, ISPA (AT); Katitza Rodríguez, Electronic Frontier Foundation (US); Tania Schroeter, DG JUST (EU)

Law enforcement authorities across the world are continuously seeking to gain access to data in different jurisdictions, wherever the data is held. Currently, the primary international mechanism for facilitating governmental cross border data access is the Mutual Legal Assistance Treaty (MLAT) process, a series of treaties between two or more States that create a formal basis for co-operation between designated authorities of the signatories. However, MLATs have been criticised for being slow and inefficient in a digital era. To fix the problems with MLATs, several government and regional proposals have emerged. This panel will explore how MLAT reform can address many current problems, as well as map different approaches to criminal investigations in the digital era in different jurisdictions to try to bring human rights to cross-border data demands, in line with human rights requirements.

- What are the proposals of the European Union on cross-border access to "e-evidence" about? What are their potential benefits and challenges?
- What is the impact of the Council of Europe negotiations on an additional Protocol to the Cybercrime Convention on national and regional initiatives?
- How is the US CLOUD Act being implemented? are there any bilateral agreements with foreign nations in the pipeline?
- Will the forthcoming UK-US surveillance agreement serve as a blueprint for other similar agreements?

17:15 – MIGRATION AND SECURITY: WHAT IMPACT ON THE RIGHTS AND FREEDOMS OF INDIVIDUALS?

Academic ** Policy ****

Organised by EDPS

Chair Giovanni Buttarelli, EDPS (EU)

Moderator Olivia Venet, LDH (FR)

Speakers Julian King, Commissioner for the Security Union (EU); Wilhelmus van Gemert, Europol (EU); Michael O'Flaherty, FRA (EU); Sergio Carrera, CEPS (BE)

DATA PROTECTION AND DEMOCRACY

COMPUTERS, PRIVACY & DATA PROTECTION

12th INTERNATIONAL CONFERENCE 30 JAN - 1 FEB 2019 BRUSSELS, BELGIUM

CPDP DATA PROTECTION 2019 AND DEMOCRACY



facebook



les halles



PLATINUM



moz://a

PREMIER



Bird & Bird



DPO Network Europe

epic.org

NYMITY
innovating compliance

OneTrust
Privacy Management Software

SQUIRE
PATTON BOGGS

Stibbe

W&G R

EVENT SPONSORS



BITS
FREEDOM



CENTER FOR
DIGITAL
DEMOCRACY

Euro★Brussels



Euro★LegalJobs

lexGO
Law jobs online

LIGA VOOR
MENSENRECHTEN
WWW.MENSENRECHTEN.BE

THE LEGAL PUBLISHER
lexxion

PRIVACY LAWS@BUSINESS
www.privacylaws.com



PRIVACY FIRST
your choice in a free society

visit.brussels

MORAL SUPPORTERS

MEDIA PARTNERS



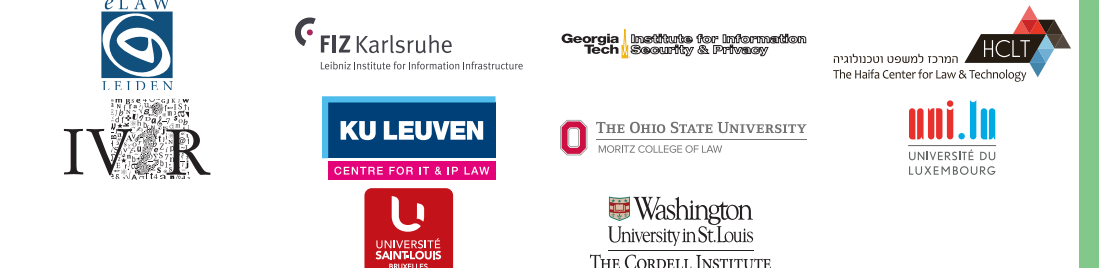
EVENT PARTNERS



EVENT PARTNERS



CONFERENCE PARTNERS



CONFERENCE PARTNERS

The EU response to the migratory crisis and security challenges relies to an important extent on Interoperability, the process of enabling large-scale EU databases to communicate and exchange information. While interoperability might prove a useful tool, it is also likely to have profound legal and societal consequences. Migration management and the fight against terrorism and organised crime are increasingly interlinked. Police are granted access to migration databases and migration authorities to police databases, new IT systems with dual purposes are under construction, and the competencies of EU agencies in the ex-third pillar sphere are being extended. In his opinion on interoperability the EDPS called for “a wider debate on the future of information sharing in the EU”. This high-level panel should give further impulse to this debate by addressing the following questions:

- Is “total information awareness” about people crossing EU borders an appropriate solution to tackle migratory and/or security challenges? At what costs in terms of individual rights? Are there alternatives?
- Under what conditions can data that have been collected for one purpose be used in a different context?
- Interoperability would inextricably link migration, police and judicial cooperation databases and impact the way legal principles have been interpreted so far in these areas. As such, it will mark a point of no return. Rather than a technical choice, interoperability is a political choice. How to ensure that the democratic process is fully complied with?

18:25 – SPEECH BY GIOVANNI BUTARELLI

Organised by EDPS

18:30 – Cocktail sponsored by EDPS in Le Village

CPDP2019 PANELS AT AREA 42 GRAND

8:45 – DPAs AND THE MEDIA

Academic ** Business ** Policy **

Organised by CPDP

Chair Charles Raab, University of Edinburgh (UK)

Moderator Ivan Szekely, Central European University (HU)

Speakers Jennifer Baker, EU Policy Correspondent (BE); Balazs Bodo, UvA (NL); Steve Wood, ICO (UK); Greet Gysen, EDPB (EU)

Media of all kinds are important players in the privacy game. Privacy and human rights-minded media can be an ally of the DPAs; others can help to spread information about the DPAs' work; but there are also numerous business and political media forums that openly criticize DP law, the GDPR and the DPAs in general. The many social and business interests around privacy, pro and con, place

articles, messages, blog posts and comments in, or aim to influence opinions through the media, as they did during the period of debates on the draft GDPR. This panel aims to explore some of these issues and relationships between DPAs and the media, focusing on questions such as:

- How do DPAs try to shape the public image of their increased authority and role under the GDPR?
- How do DPAs respond to the anti-GDPR press?
- What are the relationships between DPAs and the media of various ideological and political orientations?

10:00 – Coffee Break

10:30 – THE GDPR AND THE FREEDOM OF EXPRESSION - A ROCKY RELATIONSHIP

Academic ** Business ** Policy **

Organised by Privacy in Germany, PinG

Chair Anna Buchta, EDPS (EU)

Moderator Niko Härting, Härting Rechtsanwälte/Privacy in Germany (DE)

Speakers Olivia Tambou, Université Paris-Dauphine (FR); Bojana Bellamy, Centre for Information Policy Leadership (UK); David Erdos, University of Cambridge (UK); Paul Quinn, VUB-LSTS (BE); Horst Heberlein, DG JUST (EU)

25th May 2018 was a troubled date for many kinds of data processors. However, in particular the media - professionals (e.g. journalists) and amateurs (e.g. bloggers) - felt as if they were left out in the cold. Art. 85 GDPR leaves most of the responsibility to reconcile the right to the protection of personal data pursuant to the GDPR with the right to freedom of expression and information (Art. 11 CFR) to the member states. However, many states did little to nothing to pass specific rules to relieve the mentioned addressees. Thus, has the situation for the freedom of expression fundamentally changed? To what extent do certain rules of the GDPR enable or require a media-friendly interpretation? Which member states fulfilled their obligations to pass rules under Art. 85 GDPR? Could the lack of such rules enable a misuse of Data Protection Law that could jeopardize media freedoms? The panel will consider:

- The balance between data protection and freedom of expression after the GDPR
- New rules under Art. 85 GDPR in different Member States
- Potential jeopardy and uncertainties for press and media
- Overall effects for democracy in the EU

11:45 – CONTENT REGULATION AND ITS IMPACT ON DEMOCRACY

Academic * Business ** Policy ***

Organised by CiTiP - KU Leuven

Chair Joris Van Hoboken, VUB-LSTS (BE)

Moderator Guillermo Beltrà, Access Now (BE)

Speakers Jochen Spangenberg, Deutsche Welle/WeVerify Project (DE); Anni Hellman, DG CNECT (EU); Aleksandra Kuczerawy, CiTiP (BE); Marisa Jimenez Martín, Facebook (BE)

DATA PROTECTION AND DEMOCRACY

Internet platforms have become important fora of public debate, offering tools for increased democratic participation and engagement. The central role of internet platforms enables them to wield considerable control over online speech. Platforms effectively have the power to decide what content to disseminate and what content to remove. The same power is used to adjust content according to the profiles of users developed on the basis of their personal data. Recent scandals have shown that platforms can be misused as instruments of misinformation, propaganda and manipulation. Policy makers try to address the issue by regulating or by incentivizing platforms to adopt codes of conduct. This panel will address the impact of misinformation and content regulation on freedom of expression and democracy.

- What are the policy implications of co-opting private entities to regulate speech?
- How easy or difficult is it to recognize non-authentic content or accounts?
- Can content verification tools help address problems of misinformation?
- Are “voluntary” codes of conduct a way to circumvent the prohibition of general monitoring obligations under article 15 of the E-Commerce Directive?

13:00 – Lunch

14:15 – DATA AND ELECTIONS: AN INTERNATIONAL PROBLEM WITH NO INTERNATIONAL SOLUTION

Academic ** Business ** Policy **

Organised by Tactical Technology Collective

Chair Ravi Naik, ITN Solicitors (UK)

Moderator Elonai Hickok, Centre for Internet & Society (IN)

Speakers Ailidh Callander, Privacy International (UK); Claudio Agosti, tracking.exposed (DE); Paul Bernal, UEA School of Law (UK); Victoria Peuvrelle, Eticas Research & Consulting (ES)

There is a growing body of research into data-driven elections world-wide and the international nature of the data and elections industry has been highlighted: from international platforms, to strategists in one country advising political groups in another, to paid targeted ads across borders. Importantly, questions have arisen about the vast differences across countries in how the use of data in elections is managed and controlled.

- How important are country contexts in determining the success of regulation?
- Can technical products provide solutions to international problems that regulation can't?
- What barriers, cultural or technical, challenge international regulation?
- How can we govern organisations that change geographical status as needed?

15:30 – Coffee Break

16:00 – DIGITAL CRIME CONTROL: THE IMPACT OF PREDICTIVE POLICING ON DEMOCRACY

Academic * Business * Policy ****

Organised by CPDP

Chair Lucas Melgaço, VUB-CRiS (BE)

Moderator Frederik Zuiderveen Borgesius, Radboud University Nijmegen (NL)

Speakers Elise Lassus, FRA (EU); Lucia Sommerer, University of Göttingen (DE); Rosamunde Van Brakel, VUB-LSTS (BE); Salvatore Ruggieri, University of Pisa (IT); Sheena Urwin, Durham Constabulary (UK)

New police models are increasingly geared to predicting what will happen in the future. Two types of predictive policing are currently being implemented: predictive mapping and predictive identification. The discussion will mainly focus on the second type of predictive policing: predictive identification. Predictive identification refers to the use of new profiling technologies to predict criminal behaviour. Predictive policing raises several issues for democracy and fundamental rights. The panel will raise the following questions:

- What impact might predictive policing have on democracy?
- Does predictive policing respect the presumption of innocence?
- How should predictive policing be regulated? Is Data Protection enough? Are there technological solutions that can protect fundamental rights?
- What are the risks of unfair or illegal discrimination?

17:15 – DISINFORMATION AND ONLINE ADVERTISING: DO WE NEED TO RETHINK THE INTERNET'S BUSINESS MODEL?

Academic ** Business ** Policy **

Organised by Mozilla

Chair Sarah Eskens, UvA (NL)

Moderator Jennifer Baker, Brussels Geek (BE)

Speakers Nathalie Marechal, Ranking Digital Rights (US); Liz Carolan, Transparent Referendum Initiative (IE); Matt Rogerson, The Guardian (UK); Raegan MacDonald, Mozilla (BE)

Disinformation online and how it can be addressed is an issue that governments around the world are presently grappling with. To ensure sustainable policymaking in this space, it is essential to not just look at disinformation in isolation, but also in context of its relation to the broader internet ecosystem. This panel discussion will seek to do just that, by unpacking the relationship between disinformation and the targeted advertising business model that underpins the internet today. Bringing together a diverse panel of policy experts and practitioners, this panel will assess the sustainability of today's targeted advertising business model, and will explore whether regulatory, technological, or commercial change is needed to ensure online advertising doesn't inadvertently fuel the disinformation phenomenon.

- Which are the causes, drivers, and scope of the problem of disinformation or “information pollution”?
- What role does targeted advertising play in the spread of disinformation online?
- What role does legislation, policy, or other initiatives have in thwarting its spread?

18:30 – Cocktail sponsored by EDPS in Le Village

8:45 – USE OF PERSONAL DATA BY ONLINE PLATFORMS - DO WE STILL OWN OUR DATA?

Academic ** Business ** Policy **

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

Chair Maximilian Schrems, NOYB (AT)

Moderator Katarzyna Szymielewicz, Panoptykon Foundation (PL)

Speakers Irina Shurmina, Bryan Cave Leighton Paisner (RU); Yung Shin Van Der Syde, Timelex (BE); Ruslan Nurullaev, HSE (RU); Snezana Srdic, EDPS (EU)

Over the years, social networks, search engines, marketplaces and other online platforms accumulated vast amounts of data related to their users. GDPR entitles Internet users to access their data processed by online platforms. On the other hand, providers of new Internet services may also wish to access this data to offer their services. In practice, online platforms tend to deny full access to personal data to Internet users as well as to other businesses citing concerns over protection of their trade secrets and investments. The objective of this panel is to discuss to what extent online platforms can control the use of accumulated personal data and the information derived from such data and how the balance can be struck between the interests of online platforms, other Internet businesses and users.

- Who should have the right to claim “data ownership”: online platforms, users or both?
- How can investments of online platforms into development of user databases be adequately protected?
- To what extent should antitrust law regulate use of personal data by online platforms?
- Do online platforms have any arguments, on the grounds of GDPR, to refuse their users full access to (generated) personal data?

10:00 – Coffee Break

10:30 – DATA OWNERSHIP, INNOVATION AND PRIVACY: LOOKING FOR AN APPROACH ON BOTH SIDES OF THE ATLANTIC

Academic * Business * Policy ****

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

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

Moderator Peggy Valcke, KU Leuven (BE)

Speakers Juan Antonio Hernández Corchete, Constitutional Court (ES); Yann Padova, Baker & McKenzie (FR); Laura Schertel Mendes, Universidade de Brasília / Instituto Brasiliense de Direito Público (BR); Aurélie Pols, Data Governance & Privacy Engineer/EDPS' Ethics Advisory Group (ES/EU);

In a democratic society, it is always essential to search for the mechanisms contributing to a greater protection of citizens' fundamental rights. For years we have been witnessing a debate,

on both sides of the Atlantic, about the relevance of the formulation of a right of ownership of personal data. It is interesting to analyse how the creation of this new right has different implications in different legal systems. In this panel we will consider the following questions:

- Can the right of ownership of personal data contribute to reinforcing the right to data protection and the right to privacy?
- What would be the impact of the formulation of a right of ownership of personal data in the field of data-driven innovation? Can this right contribute to the development of technological innovations based on data?
- Can the vision based on a property right in our personal data fit in a context of the defence of a fundamental right in our democratic societies? Can personal data be an asset that may be subject to commercial and / or economic operations?
- Is the legal view about data ownership shared on both sides of the Atlantic?

11:45 – PLATFORM REGULATION

Academic ** Business * Policy ***

Organised by Research Consortium Laws of Surveillance and Security, University of Helsinki

Chair Tuomas Ojanen, University of Helsinki (FI)

Moderator Bilyana Petkova, University of Maastricht (NL)

Speakers Jennifer Daskal, American University Washington College of Law (US); Sophie Stalla-Bourdillon, University of Southampton (UK); Karmen Turk, Partner at Trinité (EE); Kamel Ajji, Paris 2 Pantheon Assas University (FR); Steven Brill, NewsGuard Technologies (US); Florent Thouvenin, University of Zürich (CH)

The rationale of the panel will be to analyze the emerging legislative and judicial responses to the evolving role of online platforms (Facebook, Twitter, other social media, blogging platforms, as well as online hosting portals and search engines). We discuss both European and American attempts to address the complex and very topical issue of intermediary regulation. The panel examines the topic in a comprehensive manner, covering terrain with recent legal developments in the U.S., in the EU Member States and at the level of the European Union and the Council of Europe.

- Is there convergence or divergence in intermediary liability between Europe (States, the EU, Council of Europe system) and the United States?
- Do we have to regulate disinformation and if so, how?
- What conclusions can we draw on platform regulation from American and European case law?

13:00 – Lunch

14:15 – CHECKS AND BALANCES IN THE AFSJ: RETHINKING GOVERNANCE

Academic * Policy *****

Organised by EDPS

Chair Wojciech Wiewiorowski, EDPS (EU)

Moderator TJ McIntyre, Digital Rights Ireland (IE)

Speakers Delphine Harou, EDPS (EU); Clara Guerra, Portuguese DPA (PT); Sophie In't Veld, MEP (EU); Christian Wiese Svanberg, Danish Police (DK)

The proposal on Interoperability calls for a wide societal debate on the governance of information exchange in the field of the AFSJ. Interoperability breaks down the borders between databases which were based on clearly defined EU policy goals (border control, security, judicial cooperation). The free flow of data creates new risks in an area where the use of personal data is opaque and may have a very significant impact on the lives and freedoms of individuals. It also challenges the current system of checks and balances. How to bring the different actors (EDPS, national DPAs, Courts and Parliaments) into a coherent governance scheme? How to ensure full accountability and to avoid blind spots, despite the blurring of the lines between national and EU level, or between AFSJ policies?

- Data subjects should be at the core of any governance scheme. How could their interests be best represented and defended in an area where data processing activities are opaque? Which role for NGOs?
- How to ensure meaningful redress and preserve accountability in a complex landscape of divided and shared responsibilities?
- Which should be the role of each administrative (DPAs/EDPS), judicial and political (EP) authority involved in the oversight?
- The cross-border (geographical and political) nature of data flows in the AFSJ calls for co-operation between the different oversight bodies. How can we ensure close collaboration while preserving the independence and role of each oversight body? Should we simplify the current supervision schemes?

15:30 – Coffee Break

16:00 – OUTSTANDING VARIABLES BEFORE THE ESTABLISHMENT OF THE EUROPEAN DATA PROTECTION SEAL

Academic * Business * Policy ****

Organised by Microsoft

Chair Irene Kamara, TILT (NL)

Moderator Hielke Hijmans, Centre for Innovation Policy Leadership (BE)

Speakers Alex Li, Microsoft (US); Andreas Mitrakas, ENISA (EU); Jelena Burnik, Slovenian Information Commissioner (SI); Isabelle Chatelier, DG JUST (EU); Willibert Fabritius, British Standards Institution (UK)

The GDPR introduces a new mechanism for certification as an element of the accountability of data controllers and processors. Certification is stipulated in Articles 42 and 43 and should play an important role in acquiring a high level of data protection. However, it is still unclear what role certification will play in practice. This is not only the case because the mechanism is new, but is also the result of the GDPR itself which leaves essential issues open. Member States, DPAs, accreditation bodies, certification bodies, the EDPB and the Commission all have to play

their role. We may expect a variety of national certifications and, at EU level, the European Data Protection Seal. Moreover, GDPR certification does not stand on its own, but closely relates to certification in, for instance, information security. This panel will discuss questions such as:

- What is the purpose of certifications and codes of conduct?
- What are the pros and cons of the different GDPR certification options and which option can better serve the underlying purpose?
- What can we learn or leverage from information security certification?
- Are there any common grounds of GDPR certification with the cybersecurity certification, stipulated in the draft EU Cybersecurity Act?
- What are the factors to consider in EC adoption of implementing and delegated acts?

17:15 – BY FAIR MEANS OR FOUL: WHAT CAN NOTIONS OF “FAIRNESS” CONTRIBUTE TO THE GOVERNANCE OF DATA PROCESSING?

Academic * Business * Policy ****

Organised by The Ohio State University Moritz College of Law

Chair Anne-Jel Hoelen, Netherlands Authority for Consumers and Markets (NL)

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

Speakers Natali Helberger, UvA (NL); Damian Clifford, KU Leuven (BE); Seda Gürses, KU Leuven (BE); Ansgar Koene, University of Nottingham (UK); Rosa Barcelo, Squire Patton Boggs (BE)

This panel will focus on the concept of fairness as a vehicle for governing data processing. It will examine how data protection law and consumer protection law utilize the notion of fairness, and explore what each can learn from the other. It will then look at how regulators, businesses and data scientists are, each in their own way, using notions of fairness to govern big data analytics and AI, and ask whether this is a helpful approach. The search is on for regulatory solutions to the risks of emerging technologies. Can the concept of fairness contribute to this quest?

- How can commitments to fairness in the GDPR and other data protection laws be used to ensure more responsible approaches to data processing and data science?
- How can a discussion of fairness from the perspective of consumer law help to inform the interpretation of fairness under GDPR, and the other way round?
- Is it possible and/or desirable to concretize the concept of ‘fairness,’ or is fairness better left defined at an abstract level?
- Provided it is possible and desirable to concretize fairness, what would be next steps that needed to happen to formalize fairness in data science and technical design?

18:30 – Cocktail sponsored by EDPS in Le Village

8:45 – PRIVACY AND DATA PROTECTION IN AFRICA: A SIMPLE TREND OR A REALITY?

Academic ** Business ** Policy **

Organised by African Network of Data Protection Authorities (RAPDP)

Chair Marguerite Ouedraogo, RAPDP (BF)

Moderator Patricia Adusei-Poku, DPC of Ghana (GH)

Speakers Omar Seghrouchni, CNDP of Morocco (MA); Sophie Kwasny, Council of Europe (INT); Boris Wojtan, GSM Association (UK); Estelle Massé, Access Now (BE)

Many African countries have enacted or are in the process of enacting privacy and data protection laws, in addition to pan African privacy regulations.

The aim of this panel is to examine the reasons behind these developments, how African privacy laws are really enforced and how they are perceived by different privacy stakeholders: do privacy laws in Africa come in response to a real need from African citizens, or it is only a trend and an imitation to countries in other parts of the world, without adaptation to local contexts.

- Are privacy and data protection a priority to African citizens? / Enacting privacy laws in Africa: a real need or a simple following of a global trend?
- What challenges must be addressed to ensure real and adequate privacy protection in Africa?
- What do we expect from privacy stakeholders in Africa (governments, regulators, the private sector, NGOs, the media)?
- What future for privacy and data protection in Africa?

10:00 – Coffee Break

10:30 – PREDICTABILITY BY PERSONAL DATA: PROFILING AND DECENCY

Academic ** Business ** Policy **

Organised by Chuo University

Chair Hiroshi Miyashita, Chuo University (JP)

Moderator Andreas Wiebe, University of Göttingen (DE)

Speakers Claire-Agnès Marnier, EDPS (EU); Winfried Veil, Data Protection Expert (DE); Sachiko Scheuing, Acxiom (DE); Monique Mann, Queensland University (AU)

This panel examines remarkable inferences from personal data: the predictability of human behavior by personal data. Personal data is often used via profiling or scoring techniques, which have been an integral part of our society for decades, to predict the future of an individual. However, the possibilities of profiling and scoring have reached a new quality. This panel explores the worst-case scenarios of algorithmic discrimination (e.g. mortgage rejections). On the other hand, the panel shares good practices by the risk-based approach in order to minimize the risks for rights and freedoms of data subjects (e.g. companies starting to effectively communicate with

their potential customers). The panel also introduces Japanese and Australian cases in comparison with the European context.

- How can we make profiling decent in terms of the risk-based approach?
- Are there gaps in profiling regulations we should mind in theory and in practice?
- What are the implications of the information bank plan in Japan and the facial-matching system and Robodebt disaster in Australia?
- Does profiling design for the AI and robotics in a privacy friendly manner?

11:45 – ISLAMIC LEGAL CONCEPTIONS OF PRIVACY

Academic ** Policy ****

Organised by CPDP

Chair Elizabeth Coombs, University of Malta (MT)

Moderator Andrew Adams, Meiji University (JP)

Speakers Nighat Dad, Digital Rights Foundation (PK); Sonny Zulhuda, International Islamic University Malaysia (MY); Omar Seghrouchni, CNDP of Morocco (MA); Patrick Penninckx, Council of Europe (INT)

Many countries with either a large majority Muslim population or an explicitly Islamic Legal system have or are considering the adoption of Data Protection legislation. This panel first presents the principles of Islamic legal theory, that laws should implement and embody principles of social organisation present in the Q'ran. The concept of privacy as presented in the Q'ran and associated commentaries follows. Finally, the implementation this leads to in example countries such as Malaysia and Indonesia is briefly described.

- How does the Q'ran figure in the development of law in Islamic countries/Muslim majority countries?
- How is privacy explicitly and implicitly present in the Q'ran?
- How is this interpreted in defining concepts of privacy for legal implementation, and how does this interpretation lend itself to abuse/misuse, e.g. in differential application to men and women?
- What differences and similarities in Data Protection exist between Muslim countries, and between Muslim and non-Muslim countries?

13:00 – Lunch

14:15 – BREACH NOTIFICATION LAWS - WHAT ARE THEY GOOD FOR?

Academic ** Business * Policy ***

Organised by University of Haifa - Faculty of Law, CCLP

Chair Anders Lindell, DG CNECT (EU)

Moderator Tal Zarsky, University of Haifa (IL)

Speakers Dennis Hirsch, Ohio State University Moritz College of Law (US); Anouk Visser, Privacy Company (NL); Lukasz Olejnik, Independent researcher & consultant (FR); Lina Jasmontaite, VUB-LSTS (BE)

Notifications of data subjects and data protection authorities in the case of specific forms of data security breaches are now mandated under the EU GDPR and all U.S. states. These laws are applauded as enhancing the rights of individuals and policing entities amassing personal data. The laws feature multiple notification requirements. They are joined by additional forms of regulations which pertain to security-related contexts and communications. Yet implementing and enforcing these rights is not without costs or consequences. Therefore, we must critically assess: what are these rules good for and how might they be improved? The panel will address the benefits, utility and costs of these regulatory requirements to individuals and organizations. It will also examine the challenges they create for regulators. After doing so, it will try to balance the related factors and consider whether there are innovative alternatives. In view of this background, the panel will consider questions such as the following:

- Under what conditions could notification policy promote cybersecurity investment?
- What, if anything, can be learned from other regulatory fields (e.g. environmental law, NIS Directive) that employ notification regimes to achieve regulatory ends?
- Will reporting fatigue substantially impact the effectiveness of notification schemes?
- How are DPAs implementing these new requirements?

15:30 – Coffee Break

16:00 – TIPS FOR DEALING WITH PERSONAL DATA BREACHES UNDER THE GDPR

Academic ** Business * Policy ***

Organised by WSGR

Chair Stewart Dresner, Privacy Laws & Business (UK)

Moderator Laura De Boel, WSGR (BE)

Speakers Barbara Radon, Zeotap (DE); Helena Koning, Mastercard (BE); Ioan Peters, Kroll (UK); Peter Eberl, DG CNECT (EU); Dina Kampouraki, EDPS (EU)

This panel will delve into the complexities of handling personal data breaches, ranging from developing a breach response plan, assessing the likelihood of risk to the rights and freedoms of individuals, to notifying data breaches to regulators and individuals. In addition, the panel will discuss expectations of regulators, emerging market practices, and strategies for managing personal data breaches in multiple jurisdictions. Join us for an exciting debate on how to navigate personal data breaches.

- How does a company prepare for a personal data breach?
- What are the expectations of regulators?
- What are the market practices regarding breach notifications?
- How does a company manage a data breach that has global implications?

17:15 – TOUCH ME, FEEL ME ... ETHICS IN A DISTANT WORLD

Academic ** Business * Policy **

Organised by CRIDS – University of Namur

Chair Christophe Lazaro, UC Louvain - JURI (BE)

Moderator Pernille Tranberg, Data Ethics (DK)

Speakers Carl Ceulemans, Royal Military School - Bruxelles (BE), Claire Lobet-Maris, University of Namur CRIDS (BE); Alain Loute, Catholic University of Lille (FR), Petra Wilson, FTI Consulting EU (BE)

The word 'touch' is the central actor of this panel. Maria Puig De La Bellacasa (2009) affirms that 'touch is world making, a thought that resonates with relational ontologies for which being is relating.' What can and does "touch" in our knowledge of the world and of others, in our perception of our responsibility and the care we owe to others? How is this touching approach of the world today modified by sensors and censors, by calculated data who mediate our relation to the world and to the others? Most of the European H2020 projects in which we are engaged promote this 'agir à distance'. They will be an opportunity to question the ethical and legal issues on these new modes of 'disincorporated' interaction with the world.

- What are the main ethical specificities of touching for relationships to others and for our engagement with the world?
- What does that mean, for our humanity, to live, work, interact with technologies that mediate and disembody our human interactions?
- Are artificial and technological developments of touch desirable to rediscover the sensation of non-mediated and corporeal relationships?
- What could it mean for the ethical assessment of technologies to think them with touch?

18:30 – Cocktail sponsored by EDPS in Le Village

CPDP2019 PANELS AT AREA 42 PETIT

8:45 – FROM LAW IN BOOKS TO LAW IN PRACTICE: GDPR COMPLIANCE CHALLENGES FOR SOFTWARE ENGINEERS AND MICROENTERPRISES

Academic ** Policy ****

Organised by PDP4E - PRiSE - SMOOTH

Chair Chris Docksey, formerly of EDPS (UK)

Moderator Edina Harbinja, Aston Law School (UK)

Speakers Massimo Attoresi, EDPS (EU); Ángel Cuevas Rumín, UC3M (ES); Kim Wuyts, KU Leuven – DistriNet (BE), Ivo Emanuilov, KU Leuven – CiTiP (BE)

There is no 'one-size-fits-all' approach when it comes to implementing GDPR. Rather, specific needs call for specific guidance. Looking at the two ends of the compliance spectrum, the panel will approach the data protection challenges faced by two key, yet very different communities: software engineers and microenterprises. While the former need methodologies and tools translating legal obligations imposed by the GDPR into technical requirements, the vulnerabil-

ities of the latter require solutions to support their compliance efforts. The panel will address the following issues:

- How can technology assist microenterprises in implementing the GDPR?
- What are the challenges of developing tool support for systematically implementing GDPR principles at the software design stage?
- Is there a room for aligning the traditional software development lifecycle with methodologies for data protection impact assessment?
- What is the role of architectural viewpoints in developing a sound data protection by design approach?

10:00 – Coffee Break

10:30 – DATA PROTECTION IMPACT ASSESSMENTS: LEGAL AND PRACTICAL CHALLENGES

Academic * Business ** Policy ***

Organised by OO&R Radboud University

Chair Stefano Leucci, Nexa Centre for Internet & Society (IT)

Moderator Mireille Hildebrandt, VUB-LSTS (BE)

Speakers Reuben Binns, Oxford University (UK); Katerina Demetrou, OO&R Radboud University (NL); Zoe Kardasiadou, EDPS (BE); Andrea Gonzalez Paz, Oracle (NL); Michael Friedewald, Fraunhofer ISI (DE)

The performance of DPIAs, in cases where the processing operations present high risks to the rights and freedoms of natural persons, is a novel legal obligation under article 35 of the GDPR. It is a promising obligation with the potential to contribute to more effective data protection - given its proactive and comprehensive nature. However, the DPIA comes with challenges. For example, the concept of 'high risk' and the assessment of identified risks in terms of 'likelihood' and 'severity' are novel in data protection. This panel will focus on the role that this obligation could play for a high level of data protection, especially in the era of algorithms and machine learning. A discussion of practical experience within the industry will substantially contribute to our understanding of challenges and potential solutions.

- What is the role of risk in the GDPR?
- What key aspects should data controllers take into consideration when building up a data protection risk management framework? Which factors may influence risk perceptions and how should risk be measured?
- Which are the lessons learned from the lists of processing operations subject to a DPIA published by the Data Protection Authorities? How is the risk to rights perceived from the perspective of the regulators?
- How could DPIAs encourage attempts to ensure fairness, anti-discrimination and procedural justice in Machine Learning (ML) applications?
- How could the assessment of the principles in Article 5 be operationalized in the DPIA process?

11:45 – PERSONALIZED LEARNING - HOW PRIVACY IS AT STAKE WHEN BIG DATA MEETS EDUCATION

Organised by CPDP

Chair Jo Pierson, VUB-SMIT (BE)

Moderator Lina Jasmontaite, VUB-LSTS (BE)

Speakers Valerie Steeves, University of Ottawa (CA); Omer Tene, IAPP (US); Priscilla Regan, Georgetown Law (US); Jen Persson, Defenddigitalme (UK)

The digitisation of learning and institutions of public education has a number of different impacts on pupils. While the use of smartphones in class is still a topic for debate in some areas, a number of major foundations in the US support the introduction of personalized learning systems into public education. These systems rely upon the collection of personal data from pupils in and out of the classroom. Algorithms then analyse the data to identify individuals' learning needs and steer their learning activities. With this panel, we examine how the meaning of learning, the role of learners and teachers, and the interplay of public and private within the educational sphere is constructed. We then analyze how general trends in the digitisation of education are likely to affect both student privacy and also education in the US and in Europe.

- How does the digital transition affect the traditional role of education?
- What are the strategies that private foundations are adopting to support personalized learning and how successful have they been?
- What impact does the digitisation of education have on the privacy of students?
- How can the emerging privacy issues be addressed?

13:00 – Lunch

14:15 – ANONYMITY LOVES COMPANY, AND FUNDING

Academic * Business ** Policy ***

Organised by University of Edinburgh

Chair Aggelos Kiayias, UEDIN (UK)

Moderator Claudia Diaz, KU Leuven (BE)

Speakers Moritz Bartl, Renewable Freedom Foundation (DE), Roger Dingledine, Tor Project (US), Harry Halpin, Inria (FR), Liz Steininger, Least Authority (DE)

Anonymity technologies differ from data confidentiality technologies in that they require a community of users that form an "anonymity set". While a pair of people can generate and use cryptographic keys to preserve the confidentiality of data, nobody can be anonymous on their own. A successful anonymity system can only provide good anonymity properties when it is used by enough people. Moreover, anonymity is rarely aligned with business incentives, online business models often rely on identifying, tracking and profiling users in exchange for personalised services and advertisements. This panel will explore these challenges and discuss:

- How do we build and sustain a community of users and developers around open source software that provides anonymity services?
- What are the best strategies for funding privacy technologies?

DATA PROTECTION AND DEMOCRACY

- Are the new applications around blockchains and cryptocurrencies an opportunity for anonymity systems?

15:30 – Coffee Break

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. Presenters:

- Teresa Quintel, University of Luxemburg (LU) - Interoperability of EU Databases and Access to Personal Data by National Police Authorities under Article 20 of the Commission Proposals
- Adam Panagiotopoulos, Trilateral Research (UK) - Genetic Information and Communities: A Triumph of Communitarianism over the Right to Data Protection under the GDPR?
- Emre Bayamlioglu, Tilburg University (NL) - Contesting Automated Decisions: A View of Transparency Implications

The jury that will comment on the papers will consist of Bart van der Sloot (Tilburg University), Maja Brkan (Maastricht University), and Mark Cole (University of Luxembourg).

Prof. Serge Gutwirth will present the award.

17:15 – SENIOR ACADEMIC SESSION 2

Academic *****

Organised by CPDP

Chair Robin Pierce, Tilburg University (NL)

Authors: Alan Rubel, University of Wisconsin-Madison (US), Clinton Castro, Florida International University (US) and Adam Pham, University of Wisconsin-Madison (US); Paula Bruening, Sequel Technology and IP Law PLLC (US) and Joshua Kroll, Princeton University (US); Arianna Rossi, University of Bologna (IT) and Monica Palmirani, University of Bologna (IT)

- Rubel et al. - Algorithmic decision systems, agency laundering, and democratic legitimacy
- Bruening and Kroll - Considering Transparency: AI, Data Science and the GDPR
- Rossi and Palmirani - On the Potentials and Limitations of Data Protection Iconography for Information Transparency

18:30 – Cocktail sponsored by EDPS in Le Village

FRIDAY 1st FEBRUARY 2019

CPDP2019 PANELS AT GRANDE HALLE

8:45 – ONLINE ABUSE OF WOMEN: WHO IS FIGHTING BACK?

Academic * Policy *****

Organised by CPDP

Chair Gloria González Fuster, VUB -LSTS (BE)

Moderator Valerie Steeves, University of Ottawa (CA)

Speakers Eva Blum-Dumontet, Privacy International (UK); Ingrid Bellander Todino, DG JUST (EU); Milena Marin, Amnesty International (UK), Rebekah K. Tromble, Leiden University (NL)

"Nameless, Faceless" (Courtney Barnett) or "Hi H8ter" (Miss Eaves) are just two examples of popular reactions to the widespread problem of online harassment of women. Harassment can take a myriad of shapes and encompass different degrees of violence and aggressiveness. It can have dramatic consequences on the lives and rights of the women affected, and it does generally perturb online debates and digital public opinion. Directly connected to sexism and misogyny, it often manifests also in connection with other discriminatory practices, and non-white women are disproportionately targeted by hateful comments and threats. The pervasiveness and insidiousness of this phenomenon triggers many questions, such as:

- What is the role of online platforms in the fight against the online abuse of women? And what could be the role of technology in measuring its incidence, as well as in countering it?
- Which framings would allow an effective fight against this, as well as against the abuse of trans and gender-diverse individuals?
- How does this problem, but also its possible solutions, intersect with the right to privacy?
- Are existing legal frameworks and European policy fit for purpose?

10:00 – Coffee Break

10:30 – PROFILING, MICROTARGETING AND A RIGHT TO REASONABLE ALGORITHMIC INFERENCES

Academic * Business ** Policy ***

Organised by Microsoft

Chair Will Scrimshaw, Microsoft (BE)

Moderator Ben Wagner, Privacy & Sustainable Computing Lab (AT)

Speakers Sandra Wachter, Oxford Internet Institute (UK); Frederike Kaltheuner, Privacy International (UK); Ravi Naik, ITN Solicitors (UK); Swati Gupta, Georgia Tech. (US)

With inferential data, conclusions can be made that extend beyond the immediate data at hand. We use for example inferential statistics to make inferences from our data to more general conditions. With more data and powerful machine learning tools, AI can magnify the ability to infer

DATA PROTECTION AND DEMOCRACY

sensitive information about us and create new data sets. Algorithmic inferences can lead to new intrusions into people's privacy and may be difficult to understand, to verify or to refute. Inferred data sets can be used for microtargeting, nudging political choices, and help to spread misinformation, with little visibility to the targets, watch dogs and oversight bodies. The use of algorithmic inferences thus can be maliciously used to encroach on democratic freedoms. European data protection laws might not sufficiently guard against these novel risks. Too much emphasis is put on data collection, very little on protection over how the data is assessed, used and shared. This panel will discuss how inferred data should be reasonably used and protected.

- What are the novel opportunities and challenges of inferential analytics?
- What are the strengths and weaknesses of European data protection law and how can we close accountability gaps?
- How can we strike a balance between privacy and transparency and business interests (IP laws, trade secrets) as well as freedom of expression?
- What governance strategies are most promising to govern inferred data, microtargeting, and the spread of misinformation?

11:45 - THE CLOUD ACT, E-EVIDENCE, AND THE GLOBALIZATION OF CRIMINAL EVIDENCE

Academic ** Business ** Policy **

Organised by Georgia Tech Institute for Information Security and Privacy

Chair Théodore Christakis, Université Grenoble Alpes (FR)

Moderator Peter Swire, Georgia Tech and Cross-Border Data Forum (US)

Speakers Cathrin Bauer-Bulst, DG HOME (EU); Ken Harris, US Department of Justice (US); Rita Balogh, Google (BE); Florence Raynal, CNIL (FR)

Since the last CPDP, the U.S. has enacted the Cloud Act, and the Commission has published its proposed E-Evidence Directive and Regulation. These law and policy changes result from a technological change – the shift to cloud computing. Evidence of crimes used to exist locally; today it is very often stored in a different jurisdiction. This panel highlights global experts on these issues, which call for: (i) responses to legitimate law enforcement requests; (ii) the need to promote privacy and human rights as essential to new legal approaches; (iii) a workable regime for companies holding the data; and (iv) risks to the global Internet from pervasive data localization.

- What are the advantages and disadvantages of the Cloud Act and E-Evidence approaches compared with Mutual Legal Assistance Treaties and European Production Orders?
- What are the advantages and disadvantages, concerning privacy and human rights protections, of the new proposed regimes? How might these protections be improved?
- What should be the role for electronic service providers in reviewing (and perhaps contesting) direct law enforcement requests under these new regimes?
- More countries have implemented (China, Russia, Vietnam) or are considering implementing (India, Indonesia) data localization requirements. To what extent can new law enforcement regimes such as Cloud Act and E-Evidence address the perceived need in these and other countries for data localization?

13:00 – Lunch

14:15 – DEMOCRACY DISRUPTED?

Academic * Business ** Policy ***

Organised by Information Commissioner's Office (ICO)

Chair Elizabeth Denham, ICO (UK)

Moderator Christian D’Cunha, EDPS (EU)

Speakers Jason Kint, Digital Context Next (US); Martin Moore, Kings College London (UK); Lisa-Maria Neudert, Oxford Internet Institute (UK); Louise Edwards, Electoral Commission (UK)

Respect for people's privacy and data about them is one of the essential freedoms underpinning a modern and vibrant demos. Attention and the civic space have been colonised by a handful of private gatekeepers which provide a easy target for malicious actors and unaccountable AI. The ensuing subversion of trust and public discourse, characterised by filter bubbles and polarisation, has led to speculation about how democracy could die. There is no quick fix for this crisis but enforcement of data protection rules is going to be integral to safeguarding fair and free participation in elections in the digital era. In election year for the European Parliament, now is the moment for regulators to join forces.

- How can democratic discourse survive in an age of 'pseudo-public' digital space?
- What is the interplay between data protection, media and electoral rules and how should regulators coordinate enforcement?
- What role for antitrust in disciplining dominant platforms and preventing further concentration of informational power
- What in practical terms is needed to bolster the integrity of the EP elections in 2019?

15:30 – Coffee Break

16:00 – SURVEILLANCE CAPITALISM AND REGULATORY CAPTURE? • THE CASPAR BOWDEN PANEL

Academic ** Business ** Policy **

Organised by CPDP

Chair Paul De Hert, VUB-LSTS (BE)

Moderator Giovanni Buttarelli, EDPS (EU)

Speakers Shoshana Zuboff, Harvard Business School (US); Julie Cohen, Georgetown Law (US); Gary Davis, Apple (IE); Andrea Renda, CEPS (BE)

The commodification of personal data as a result of technological innovations is of a magnitude and ubiquity that qualifies as a defining societal condition and signals the onset of a new era: Surveillance Capitalism. To Shoshana Zuboff “this new form of information capitalism aims to predict and modify human behavior as a means to produce revenue and market control.” Naturally, surveillance capitalism can function best in social contexts adapted to its needs. In this regard, this panel will consider the extent to which surveillance capitalism - as a mode of thought and action - has succeeded in infiltrating and capturing democratic and legislative processes

and shaping them to its purposes.

- In what ways does surveillance capitalism infiltrate democratic and legislative processes?
- How far has this infiltration gone?
- Where is it heading in the future?
- What are the alternatives and how might resistance best be mounted?

17:15 – Closing Remarks by Giovanni Buttarelli in Grande Halle

CPDP2019 PANELS AT AREA 42 GRAND

8:45 – ENSURING DOMAIN NAME DATA IS SAFE: THE WHOIS EXPERIENCE OF BALANCING CYBERSECURITY AND PRIVACY NEEDS IN THE ERA OF GDPR AND MAJOR EVOLUTION OF PRIVACY LEGISLATION AROUND THE WORLD

Academic ** Business ** Policy **

Organised by Internet Corporation for Assigned Names and Numbers/ICANN

Chair Adam Peake, ICANN (INT)

Moderator Joanna Kulesza, University of Lodz (PL)

Speakers Caroline Greer, Cloudflare (IE); Elena Plexida, ICANN (INT); Grégory Mounier, Europol (EU); Walter van Holst, EDRi (NL); Peter Van Roste, CENTR (BE); Cristina Monti, DG JUST (EU)

The panel will focus on the challenge of ensuring consistency between local and regional legal frameworks with global policies underpinning the Internet such as implementing the GDPR for the purposes of the Internet domain name industry. Discussions will highlight the challenge of identifying “legitimate interests” for processing domain name data and the decades long dilemma of the WHOIS database, under significant change subject to GDPR implementation by the Internet Corporation for Assigned Names and Numbers (ICANN). The panel will serve to highlight ICANN’s efforts to comply with GDPR and its unique multistakeholder process behind developing the relevant policy. It will reflect the broad lessons learned on global multistakeholder processes responding to regional legislation. In particular the panelists will highlight the work on accrediting access to personal data of domain name registrants.

- How does ICANN WHOIS policy impact Internet users and global standards for privacy and data protection?
- How is ICANN’s global multistakeholder process responding to GDPR as regional legislation?
- How to balance legitimate interests in accessing data in a global multistakeholder environment?
- What are the lessons learned for Internet policy development, global MS processes and the trend towards national and regional legislation effecting the Internet?

10:00 – Coffee Break

10:30 – LOOKING BACK FOR FUTURE LESSONS

Academic * Policy *****

Organised by Tilburg Institute for Law, Technology, and Society - TILT

Chair Ronald Leenes, TILT (NL)

Moderator Gloria González Fuster, VUB-LSTS (BE)

Speakers Peter Blok, Universiteit Utrecht (NL), Colette Cuijpers, TILT (NL), Nadezhda Purtova, TILT (NL), Claudia Quelle, TILT (NL), Ivan Škorvánek, TILT (NL)

The past 25 years we have witnessed a lot of social, technical and legal changes and challenges in the landscape of privacy and data protection. The Tilburg Institute for Law, Technology, and Society is celebrating its 25th anniversary in 2019. We look back on many years of privacy and data protection research, laid down in many research reports, journal articles, books and dissertations. In this panel we will guide the audience through 25 years of academic research by (former) TILT researchers. We want to reflect upon 25 years of Privacy and Data Protection development and want to see how the landscape has changed, if fundamentals still hold strong and if and how lessons from the past can help develop the privacy and data protection landscape for the next 25 years.

- Which lessons can be learned from Data Protection frameworks preceding the GDPR?
- Is there a role to play for private law and property law approaches?
- Has the concept of privacy changed over time?
- Does a risk-based approach provide the answers to current Data Protection challenges?

11:45 – TECHNICAL STANDARDS ON ETHICS AND/OR REGULATION?

Academic * Business * Policy ****

Organised by IEEE

Chair Marit Hansen, ULD (DE)

Moderator Paul Nemitz, DG JUST (EU)

Speakers Sarah Spiekermann, WU Vienna (AT); Alan Winfield, UWE Bristol (UK); Kai Rannenberg, University of Frankfurt (DE); Alessandro Guarino, CEN/CENELEC (BE)

Standards will determine HOW regulation is lived, what informed consent will look like concretely, how transparency of algorithms and data processing are to be lived concretely, what measures are necessary to avoid system bias or what it means to certify for an “ethics by design” label. The coming battle for privacy and ethics is around the standards in the making. Therefore, major standardization organizations have entered the scene; setting up technical and organizational standards addressing ethical concerns in system design. Amongst them, most prominently, IEEE with its IEEE’s Global Ethics Initiative. IEEE is not the only standardization organization active in this field. ISO/IEC and CEN/CENELEC are equally active in the domain, albeit not necessarily under the headline of ethics.

- What is the interplay between regulation and technical standards in the field of digital privacy and ethics?
- How powerful are standards in the field of privacy and ethics?

DATA PROTECTION AND DEMOCRACY

- What are the political challenges encountered in the building of standards?
- Should standards driven by ethical concerns replace regulation or are they complementary to the law?

13:00 – Lunch Break

14:15 – CLASHING CONSTITUTIONAL NORMS, CROSS-BORDER DATA, AND FREE EXPRESSION

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

Chair Neil Richards, Washington University (US)

Moderator Jennifer Daskal, American University Washington College of Law (US)

Speakers Kirsty Hughes, Cambridge University (UK); Gavin Philipson, Durham University (UK); Lorelein Hoet, Microsoft (BE); Lanah Kammourieh Donnelly, Google (UK)

This panel will examine challenges posed by competing speech and privacy norms across borders, the cross-border consequences of local efforts at control, and possible means for resolving disputes. In particular, the panel will examine the proliferation and implications of transfer restrictions on data, high-profile court cases addressing the geographic reach of takedown and delisting orders, and the cross-border effects of and responses to fake news, both by governments and technology companies. The panel will focus primarily on the EU and US, although the discussion will have broader implications for parallel efforts and disputes playing out in various locations across the globe.

- What are the differences in free speech rights and privacy rights between the US and EU?
- What are the origins of these differences?
- How if at all can these differences be resolved?
- What can companies and individuals do when faced with competing legal rules?

15:30 – Coffee Break

16:00 – CyberBRICS: CHALLENGES AND OPPORTUNITIES FOR DATA PROTECTION IN THE BRICS

Academic ** Business * Policy ***

Organised by Fundação Getulio Vargas Law School

Chair Hannah Draper, Open Society Foundations (CA)

Moderator Luca Belli, FGV Law School (BR)

Speakers Danilo Doneda, Brazilian Institute for Public Law (BR); Alexey Ivanov, HSE-Skolkovo Institute for Law and Development (RU); Elonnai Hickok, Centre for Internet and Society (IN); Marcelo Thompson, University of Hong Kong (CN); Ian Brown, Research ICT Africa (UK)

BRICS are developing or enacting data protection frameworks that will soon affect almost 50% of the world's population and almost 40% of existing Internet users, who live in the BRICS.

This session is part of the CyberBRICS project, which explores data protection and cybersecurity frameworks in the BRICS. Panellists will analyse the advancements and challenges regarding

BRICS data protection frameworks, focusing on:

- The approval of a new "General Data Protection Law", in Brazil;
- The enactment of data protection and data localisation provisions, in Russia;
- The Indian Supreme Court recognition of privacy as a fundamental right and the consultations on a new Indian Data Protection Bill;
- The current consultation on the new "Internet Personal Information Security Protection Guidelines", in China;
- The partial enactment of the "Protection of Personal Information Act", in South Africa.

17:15 – Closing Remarks by Giovanni Buttarelli in Grande Halle

CPDP2019 PANELS AT PETITE HALLE

8:45 – FAIRNESS BY DESIGN: ETHICS AND DATA PROCESSING IN RESEARCH CONTEXT - CAN WE SAFEGUARD FUNDAMENTAL HUMAN RIGHTS IN THE DIGITAL WORLD?

Organised by European Centre on Privacy and Cybersecurity (ECPC), Maastricht University

Chair Cosimo Monda, Maastricht University (NL)

Moderator Paolo Balboni, ICT Legal Consulting (IT)

Speakers Aurélie Pols, Data Governance & Privacy Engineer/EDPS' Ethics Advisory Group (ES/EU); Michel Dumontier, Maastricht University (USA/NL); Albena Kuyumdzhieva, DG Research and Innovation (EU); Giovanni Comandé, Scuola Superiore Sant'Anna (IT); Martin Abrams, The Information Accountability Foundation (US)

The new technological developments have brought enormous research possibilities and have enabled rapid science advancements, by supplying the research community with tools for collecting, storing, merging and analysing enormous amounts of data in ways that were unimaginable just a few years ago. These advancements however can sometimes come at a price to 'ethics' and can challenge the implementation of some basic fundamental rights. The GDPR recognises the importance of technological development for the benefit of the digital society and sets forth special rules to carry out data processing for research purposes. This panel focuses on how the new data protection rules will determine and affect the use of personal data for research purposes and how to pursue an ethical approach to data processing through the implementation of "fairness-by-design" into automated decision-making.

- Can we safeguard fundamental human rights in the digital world?
- What are the implications of the new data protection rules when using personal data for research purposes?
- How to pursue ethical data processing through the implementation of "fairness-by-design"?

DATA PROTECTION AND DEMOCRACY

10:00 – Coffee Break**10:30 – DATA AND RELIABILITY: MORE IS MORE OR MORE IS LESS?****Academic *** Business * Policy ******Organised by** Centre for Law and Digital Technologies of Leiden University/eLaw**Chair** Ioulia Konstantinou, VUB-LSTS (BE)**Moderator** Francien Dechesne, Leiden University (NL)**Speakers** Geert-Jan de Koning, IBM (NL); Karolina La Fors, Leiden University (NL); Antti Yogi Poikola, MyData Platform (FI); Bryan Ford, Swiss Federal Polytechnic University (CH)

In our big data intensive society and economy, more data came to mean more value, arguably because it leads to more reliable predictions about both natural individual and societal processes. However, practice shows that the more society comes to rely on big data systems, the more vulnerable we become when those systems are actually not reliable (enough). With the panel, we want to highlight the importance of reliability of both technical and societal systems and how they can interact. In particular we aim to generate discussion about the reliability of digital identities. The following, in particular, will be discussed:

- How to find legal, technological and societal solutions for improving the reliability of personal data that establish a personal identity?
- How to find legal, technological and societal solutions for improving the reliability of systems using these identities?
- How to find legal, technological and societal solution for tackling systems and processes that undermine the reliability of personal identities and their use?

11:45 – NEW DATA PROTECTION REGULATION FOR EU INSTITUTIONS AND BODIES - ANOTHER PIECE OF THE PUZZLE**Academic ** Business * Policy *******Organised by** CPDP**Chair** Cornelia Ernst, MEP (EU)**Moderator** Vagelis Papakonstantinou, VUB-LSTS (BE)**Speakers** Diana Alonso Blas, Eurojust (EU); Elena Gil Gonzalez, CEU San Pablo University/IVIR (ES/NL); Juraj Sajfert, DG JUST (EU); Christina Samaras, Cleary Gottlieb Steen & Hamilton LLP (FR); Wojciech Wiewiorowski, EDPS (EU)

On 11 December 2018, almost two years after the Commission presented its proposal, the new data protection Regulation for Union institutions and bodies (EU) 2018/1725 entered into application, replacing the Regulation (EC) No 45/2001. The new Regulation aligns the data protection regime for Union institutions and bodies with the GDPR and the Data Protection Law Enforcement Directive (EU) 2016/680. At the same time, and after five years of legislative negotiations, the new Eurojust Regulation entered into force and will apply from 12 December 2019. With these two brand new legislative instruments, in 2019 Eurojust will become the first EU law enforcement agency that does not have an autonomous, standalone data protection regime.

- What is the meaning of all these changes? Why a separate Regulation for Union institutions and bodies?

- What are the differences between the new Regulation and the GDPR/Data Protection Law Enforcement Directive?
- What are the EU law enforcement agencies? Do e.g. Frontex or the EU Common Defense and Security Policy missions have law enforcement tasks? What is a law enforcement task?
- Do EU law enforcement agencies need even more specific data protection rules than the GDPR/Data Protection Law Enforcement Directive, and if yes, why?

13:00 – Lunch**14:15 – TO PORT OR NOT TO PORT? UNDERSTANDING THE LIMITS AND BENEFITS OF DATA PORTABILITY****Academic ** Business ** Policy ******Organised by** Future of Privacy Forum**Chair** Thomas Zerdick, EDPS (EU)**Moderator** Stacey Gray, FPF (US)**Speakers** Joris Van Hoboken, VUB-LSTS/UvA (BE/NL); Gabriela Zanfir-Fortuna, FPF (US); Babak Jahromi, Microsoft (US); Olivier Micol, DG JUST (EU)

The Cambridge Analytica downfall shows the importance of platforms limiting access of third parties to the personal data they hold. However, such limitations cannot be absolute. As a matter of fact, one of the biggest innovations of the GDPR is the introduction of data portability as a new right of the data subject. Data portability presupposes that new players on the market, from a small gaming app to an ambitious new platform facilitating exchange of information, should have access to personal data of an individual collected and amassed by their competitors or by any other player in a different market, if the individual so wishes.

- How should organizations implement portability to maximize individual rights?
- What is the relationship between ensuring portability and platforms exercising responsible oversight of the activity of apps?
- Is portability a right that advances competition to support diverse options for individuals, or an individual data protection right that incidentally supports competition and does it matter?
- In addition to data protection authorities, what role will codes, independent watchdogs, self-regulation, civil society, media or other efforts play to ensure third party access to data via portability is not abused?

15:30 – Coffee Break**16:00 – ‘PURPOSE LIMITATION IS DEAD, GET OVER IT’ ON THE UNDERMINING OF DATA PROTECTION LAW****Academic **** Policy ******Organised by** Vrije Universiteit Amsterdam**Chair** Arno Lodder, SOLV Advocaten (NL)**Moderator** Magdalena Jozwiak, Vrije Universiteit Amsterdam (NL)**Speakers** Teresa Quintel, University of Luxembourg (LU); Tijmen Wisman, Platform for the**DATA PROTECTION AND DEMOCRACY**

Protection of Civil Rights (NL); Fanny Coudert, EDPS (EU); Judith Rauhofer, University of Edinburgh (UK)

Purpose limitation is one of the cornerstones of data protection law. It can be considered a bulwark for privacy in the 'datafied' society. Purpose limitation is closely linked to the rule of law and specifically foreseeability, because it (originally) imposed limits on the competence of public authorities to process data beyond their legal mandate. It is the principle which protects the contextual confidentiality in which personal data is processed and prevents the unforeseen use of data against a person. The aim of this panel is to create an overview of the recent and planned changes to the purpose limitation principle in EU data protection laws in order to discuss the implications of these changes for data protection law as a substantive limit on the power of government.

- Purpose limitation is one of the cornerstones of data protection law, imposing substantive limits on the powers of government
- What are the current and planned amendments of the purpose limitation principle in EU data protection laws?
- What policy changes concerning data analytics are these amendments facilitating?
- What are the implications of these changes for the fundamental rights and freedoms of citizens?

17:15 – Closing Remarks by Giovanni Buttarelli in Grande Halle

CPDP2019 PANELS AT LA CAVE

8:45 – E-GOVERNMENT, DIGITAL IDENTITY AND DATA PROTECTION: HOW TO ENGINEER DATA PROTECTION PRINCIPLES FOR E-ID SCHEMES?

Academic ** Policy ** Business **

Organised by FutureTrust

Chair Caroline Louveaux, Mastercard (BE)

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

Speakers Marc Sel, PwC (BE); Mark King, EEMA (UK); Niko Tsakalakis, University of Southampton (UK); Eric Verheul, KeyControls (NL)

An observable trend in eGovernment initiatives throughout Europe in recent years has been the emergence and rollout of electronic identity (eID) schemes that allow individuals to manage and authenticate their identities in conjunction with the use of online public services. The development of national eID schemes can also be situated in the context of the encouragement of the deployment of eID schemes at the EU level with the adoption two years before the GDPR of the Regulation on electronic identification and trust services for electronic transactions in the inter-

nal market (eIDAS). eIDAS defines an interoperability framework for national eID schemes, which should 'facilitate' data protection by design. It is however not clear what the implications of GDPR Art. 25 should be for eID schemes.

- What should the implications of GDPR Art. 25 be for national eID schemes?
- How will the eIDAS interoperability framework impact upon the level of data protection guaranteed by national eID schemes?
- How to demonstrate data protection by design for eID schemes?
- What are the implications of the push for expanding the use of eID schemes to enable access to private services?

10:00 – Coffee Break

10:30 – LAW ENFORCEMENT WITHOUT BORDERS: ACCESS TO ELECTRONIC DATA UNDER THE EU PRODUCTION ORDER AND THE US CLOUD ACT

Academic * Business * Policy ***

Organised by CEPS

Chair Marco Stefan, CEPS (BE)

Moderator Jason Biros, VUB-LSTS (BE)

Speakers Kenneth Harris, United States Department of Justice (US); Anze Erbeznik, LIBE Secretariat (EU); Etienne Maury, CNIL (FR); Laure Baudrihay-Gérard, Fair Trials Europe (BE); Alexandra Laffitte, EuroISPA (AT)

Crime fighting within Europe and across the Atlantic increasingly relies on the possibility to access electronic information held by IT Service Providers. The EU and the US are equipping Law Enforcement Authorities (LEAs) with new tools that will speed up the gathering of data located outside of their countries' territory. The European Production and Preservations Orders, as well as the US CLOUD Act will allow investigating and prosecuting authorities to seek data directly from private companies, regardless of their location. But is the Internet really borderless? This Panel explores the conflicts of laws that might arise when LEAs seek to obtain data which are subject to foreign jurisdictions.

- Which are the main challenges that the implementation of the US CLOUD Act poses from an EU primary and secondary law perspective?
- Will the European Production and Preservation Orders prevent or increase conflicts of law between the EU and the US?
- Are Mutual Legal Assistance Treaties still a valid channel for criminal justice cooperation in the gathering of electronic information?

11:45 – CIVIL SOCIETY AND THE COLLECTIVE REDRESS OF DATA PROTECTION HARMS

Academic ** Business * Policy ***

Organised by Internet Society France

Chair Maryant Fernández Pérez, BEUC (BE)

DATA PROTECTION AND DEMOCRACY

Moderator Julien Rossi, Université Rennes 2 (FR)

Speakers Lucien Castex, Internet Society France / Université Sorbonne Nouvelle (FR), Alexis Fitzjean Ó Cobhthaigh, La Quadrature du Net (FR), Karolina Iwańska, Panoptikon Foundation (PL); Nick McAleenan, JMW Solicitors Manchester (UK), Jennifer Salat, DPO Circle (BE)

The GDPR has introduced new collective redress mechanisms in the field of data protection. In some EU member states, it is even possible to sue for compensation in the frame of such collective action, and many civil society organisations have already seized this opportunity. How do we quantify harm related to the violation of data protection rights? Does the violation of a procedural obligation by a data controller, such as the obligation to maintain a register of processing operations, constitute reparable damage? Or does the law only provide for the possibility to sue for damage that was the consequence of such a violation? We will discuss all of this and more in this session, including the state of play of some of the collective action initiatives and the reaction of data controllers.

- What is the state of play of the implementation of art. 80 GDPR especially with regards to collective redress mechanisms?
- How to quantify harms when it comes to asking for compensation for the violation of data protection rights?
- Have collective redress mechanisms changed the landscape of data protection in Europe?
- What happens in cross-border situations where collective redress actions meet the one-stop-shop mechanism?

13:00 – Lunch

14:15 – LOST IN COOPERATION? CROSS-BORDER COMPLAINTS PROCEDURES IN PRACTICE

Organised by NOYB

Chair Ioannis Kouvakas, NOYB (AT)

Moderator Jack Parrock, Feature Story (BE)

Speakers Maximilian Schrems, NOYB (AT); Herwig Hofmann, Uni Luxembourg (LU); William Malcolm, Google (UK); Isabelle Vereecken, EDPB (EU); Francisco Enrique González-Díaz, Cleary Gottlieb Steen & Hamilton LLP (BE)

One of the most innovative changes in GDPR was the establishment of cross-border cooperation. But how does this work in practice? How can DPAs that are subject to more than 30 different national or local procedural laws run a joint procedure in compliance with the controller's and data subjects' rights? In that respect, the role of the national legislation implementing the GDPR will also be examined. Finally, the debate will touch upon the EDPB competence to take over a case when there is a disagreement between the DPAs, possible competence in cases of non EU controllers, what the rights of the data subjects are in such situations and what the role of the European courts will eventually be.

- How can supervisory authorities comply with multiple procedural laws in cross-border complaints?

- Can data subjects' procedural rights be adequately enforced in a pan European landscape?
- What is the role of the EDPB when it comes to cooperation among supervisory authorities?
- What is the role of the CJEU as an ultimate interpreter of the GDPR?

15:30 – Coffee Break

16:00 – CLOSED SESSION

17:15 – Closing Remarks by Giovanni Buttarelli in Grande Halle

CPDP2019 PANELS AT AREA 42 PETIT

8:45 – THE IMPACT OF THE GDPR ON HEALTH RESEARCH PRACTICES

Academic * Business ** Policy ***

Organised by BBMRI-ERIC

Chair Isabelle Huys, University of Leuven (BE)

Moderator Michaela Th. Mayrhofer, BBMRI-ERIC (AT)

Speakers Gauthier Chassang, INSERM (FR); Victoria Chico, Health Research Authority (UK); Olga Tzortzatou, Bioacademy (GR); Tom Southerington, University of Turku (FI)

The EU General Data Protection Regulation may have significant implications for data protection practices of researchers and donor involvement. Especially so as the regulation provides space for national and EU-level derogations and specifications in areas such as scientific research. This panel aims to assess the practical consequences of the GDPR for data sharing within the EU with regards to biomedical research, especially biobanking.

- How does the GDPR impact health research in general in the EU?
- What are the main changes in contrast to the Directive?
- How do country derogations influence cross-border data sharing?
- What is the preferred legal basis for processing personal data for research?

10:00 – Coffee Break

10:30 – THE USE OF BIG HEALTH DATA IN RESEARCH

Academic * Business ** Policy ***

Organised by VUB-LSTS

Chair Paul Quinn, VUB-LSTS (BE)

Moderator Robin Pierce, TILT (NL)

Speakers Joan Antokol, Park Legal LLC (US); Dara Hallinan, FIZ Karlsruhe (DE); Liam Quinn, UCL (UK); Amanda Cole, EFPIA (BE)

The use of big data is becoming central to many forms of scientific research. The use of big

health data in particular presents vast opportunities for researchers whilst at the same time presenting many challenges, not least in the area of privacy and data protection. This panel will focus on these challenges and analyse what problems they may pose for the future of research with 'big health data'. It will include perspectives from scientific researchers (related to computational genetics), biobanking and the pharmaceutical industry. The aim will be to present a balanced and varied perspective of how data protection laws can facilitate and hinder research using 'big health data'.

- Why does data protection present problems for research with big health data?
- How do data protection requirements impact on researchers using big genetic data?
- How do they affect the use of big health data in biobanking?
- To what extent does data protection law allow big data to be assembled from secondary data for research purposes?

11:45 – HEALTH DATA AND AI IN CLINICS AND RESEARCH: LEGAL BASIS, TRANSPARENCY AND ACCOUNTABILITY

Academic ** Business ** Policy **

Organised by PANELFIT and Brussels Privacy Hub

Chair Albena Kuyumdzhieva, DG Research and Innovation (EU)

Moderator Gianclaudio Malgieri, Brussels Privacy Hub (BE)

Speakers Bernd Stahl, De Monfort University (UK); Zuzanna Warso, Helsinki Foundation for Human Rights (PL); Nicola Orlandi, Novartis (CH); Aliuska Duado, University of the Basque Country (ES)

The panel will discuss the key challenges of health data processing in clinics and research under the GDPR and beyond: in particular, how to balance the protection of patients/data subjects with the interests of medical research. Relevant elements to consider are lawfulness, transparency and accountability. As regards lawfulness, it is necessary to explore the limits of informed and free consent (in particular in the case of data monetisation or where secondary data subjects are involved) and the opportunities to avoid consent requests (e.g. because of "public interests"). As regards transparency and accountability, a key challenge is the balancing between right to access (in particular when AI technologies are used) and public or private interests behind research. Some practical solutions will also be discussed, e.g. the helpfulness of DPIA or code of conducts in this field.

- How to deal with risks of using of new data-mining techniques in the context of clinics and how to protect rights and freedoms of data subjects?
- It is well known that in the context of biomedical research there is a conflict between private and public interest. How should it be assessed in terms of data protection law?
- What are the main ethical, legal and governance issues related to AI in the health care context? How could we solve them?

13:00 - Lunch Break

14:15 – INSURANCE, ALGORITHMIC DECISION-MAKING, AND DISCRIMINATION

Academic ** Business * Policy ***

Organised by CPDP

Chair Jędrzej Niklas, University of Leeds (UK)

Moderator Frederik Zuiderveen Borgesius, IViR Institute for Information Law (NL)

Speakers Toon Calders, University of Antwerp (BE); Ursula Pachi, BEUC (BE); Freyja Van Den Boom, Bournemouth University (UK); Jos Schaffers, Dutch Association of Insurers (NL)

Insurance companies could use algorithmic systems to set premiums for individual consumers, or deny them insurance. More and more data become available for insurers for risk differentiation. For instance, some insurers monitor people's driving behaviour to estimate risks. To some extent, risk differentiation is necessary for insurance. And it can be considered fair when high-risk drivers pay higher premiums. But there are drawbacks. Algorithmic decision-making could lead, unintentionally, to discrimination on the basis of, for instance, skin colour. And too much risk differentiation could make insurance unaffordable for some consumers, and could threaten the risk-pooling function of insurance. Furthermore, risk differentiation might result in the poor paying more. A consumer who lives in a poor neighbourhood with many burglaries might pay more for house insurance, because the risk of a burglary is higher. Hence, poor people might pay, on average, more.

- How should discrimination on the basis of, for instance, skin colour be avoided?
- Can non-discrimination norms be built in the computer systems of insurance companies?
- Are current laws sufficient to protect fairness and the right to non-discrimination in the insurance area?
- Should the law protect poor people against paying extra?
- Is it always reasonable when high-risk insurance consumers pay extra?

15:30 – Coffee Break

16:00 – CLOSED SESSION

17:15 – Closing Remarks by Giovanni Buttarelli in Grande Halle

CPDP2019 Side Events

THE AGE OF SURVEILLANCE CAPITALISM

THE FIGHT FOR A
HUMAN FUTURE
AT THE NEW
FRONTIER OF POWER

SHOSHANA
ZUBOFF

CPDP2019 OPENING NIGHT: BOOK LAUNCH OF SHOSHANA ZUBOFF'S "THE AGE OF SUR- VEILLANCE CAPITAL- ISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER"

Date 29/1/2019 19:00

Organised by Privacy Salon & VUB-LSTS

Location Les Halles de Schaerbeek, Rue Royale-Sainte-Marie 22, 1030 Schaerbeek

Shoshana Zuboff will present her latest book, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power". This new work integrates Zuboff's lifelong themes: the historical emergence of psychological individuality, the conditions for

human development, the digital revolution, and the evolution of capitalism. It begins with the oldest questions: home or exile? master or slave? It explores the emergence of surveillance capitalism as the dominant form of information capitalism and its implications for individuals, society, and democracy in the twenty-first century.

With **Francesca Bria**, City of Barcelona/Decode Project (ES), **Paul Nemitz**, European Commission DG Justice (EU), **David Murakami Wood**, Surveillance Studies Centre, Queens University (CA) and **Shoshana Zuboff**, Harvard Business School (US). **John Naughton**, University of Cambridge/The Observer (UK) will be moderator.

DIGITAL DATA FLOWS MASTERCLASS: DE-IDENTIFICATION

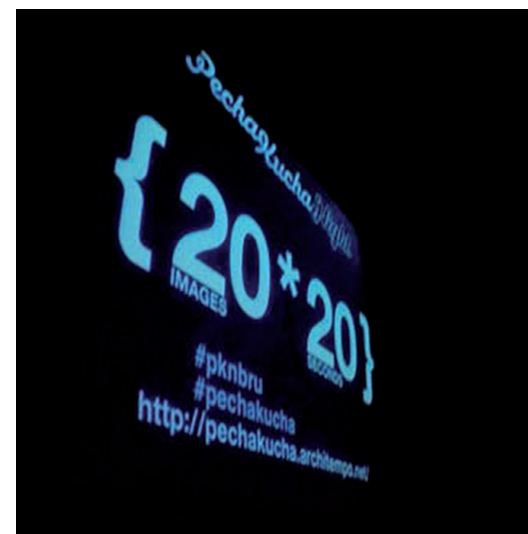
Date 30/1/2019 14:00 - 15:30

Organised by Future of Privacy Forum and Brussels Privacy Hub

Location Area 42 - Room A, Rue des Palais 46, 1030 Brussels

Digital Data Flows Masterclass is a year-long educational program designed for regulators, policymakers, and staff seeking to better understand the data-driven technologies at the forefront of data protection law & policy. The program will feature experts on machine learning, biometrics, connected cars, facial recognition, online advertising, encryption, and other emerging technologies. Register here: www.fpf.org/classes

COMPUTERS, PRIVACY & DATA PROTECTION



PECHAKUCHA

Date 30/1/2019 20:20 - 22:30

Organised by Architempo & Privacy Salon

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

More Information <http://pechakucha.architempo.net>

10 speakers, each speaker has 6 minutes 40 seconds for a presentation in 20 images. Each image is onscreen 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.

DATA PROTECTION AND DEMOCRACY

Dance like no one is watching The official CPDP party

Mozilla invites you to join us in raising a glass for privacy in the digital age at the CPDP party

Drinks, nibbles & good times

From 20:00 on Thursday at Area 42

See you there!

moz://a

DANCE LIKE NO ONE IS WATCHING: THE OFFICIAL CPDP PARTY!

Date 31/1/2019 20:00 - 24:00

Organised by Mozilla

Location Area 42, Rue des Palais 46, 1030 Brussels

Mozilla invites to you join us in raising a glass for privacy in the digital age at the CPDP party.

Drinks, nibbles & good times. See you there!

Privacytopia Artistic Programme



MEGAPIXELS: WHO IS IN PUBLICLY AVAILABLE FACIAL RECOGNITION DATASETS?

Date 30/1/2019 17:15 - 18:30

Organised by Privacy Salon

Location Area 42, Rue des Palais 46, 1030 Brussels

With Adam Harvey, Seda Gürses & Ben Hayes

Artist and researcher Adam Harvey will debut a new chapter of the MegaPixels project, an investigation into the origins and ethics of facial recognition training datasets. What many Internet users might not yet know is that many facial recognition datasets are created from social media posts, Flickr albums, Instagram, and Google searches of public figures. Facial recognition only works when there is enough training data and much of that data is generated by Internet users. But many of these datasets disappear from the public view once they are created. The MegaPixels project is building a new facial

recognition API that helps you search these datasets for your image in order to challenge. Looking beyond the actual facial images, the project also explores the origins and digital trade routes and the complexities of unregulated international facial data exchange.

FACELESS: RE-INVENTING PRIVACY THROUGH SUBVERSIVE MEDIA STRATEGIES

Date 31/1/2019 16:00 - 17:15

Organised by Privacy Salon

Location Area 42, Rue de Palais 42-46, 1030 Brussels

With Bogomir Doring, Gloria González Fuster & Paul de Hert

Artist, researcher and curator Bogomir Doring (Artistic Research PhD, University of Applied Arts Vienna) will present his on-



COMPUTERS, PRIVACY & DATA PROTECTION

going project FACELESS that was recently published by de Gruyter. The book is: "Faceless: Re-inventing Privacy Through Subversive Media Strategies". The project looks into a ritual of masking, attached to creative arts in contemporary post-9-11 society. The contributions to this book explore a phenomenon that appears to be a contradiction in itself – we, the users of computers, can be tracked in digital space for all eternity. Although, on the one hand, one wants to be noticed and noticeable, on the other hand, one does not necessarily want to be recognized at the first instance, being prey to an unfathomable public, or – even less so – to lose face. The book documents artistic and other strategies that point out options for appearing in the infinite book of faces whilst nevertheless avoiding being included in any records. The desire not to become a mere object of facial sell-out does not just remain an aesthetic endeavour. The contributions also contain combative and sarcastic statements against a digital dynamic that has already penetrated our everyday lives.

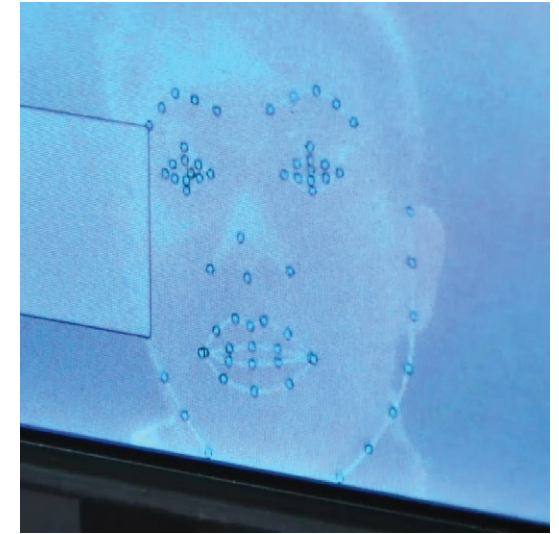
Image Cover © by Lisette Appeldorn for the book Faceless: Re-inventing Privacy Through Subversive Media Strategies

ARTWORKS ON VIEW IN AREA42

ARCHIVING FACELESS – A film by Bogomir Doring, edited by Rafael Kozdron

ALGO-RHYTHM – A film musical against Automated Propaganda directed by Manu Luksch, starring Gunman Xuman, Lady Zee and OMC
THINK PRIVACY posters by Adam Harvey

DATA PROTECTION AND DEMOCRACY



QUANTIFICATION WILL TEAR US APART

Date 31/1/2019 17:15 - 18:30

Organised by Privacy Salon

Location Area 42, Rue des Palais 46, 1030 Brussels

With Manuel Beltrán, Katarzyna Szymielewicz & Rocco Bellanova

Artist, activist and founder of the Institute of Human Obsolescence (IoHO) Manuel Beltrán will present his ongoing research into the contemporary quantified condition. The IoHO explores the socio-political and economic implications of technology in a society in which the relationship between humans and machines is dramatically changing.

Modern societies impose quantification in all aspects of humans' lives. This talk explores how this phenomenon is enabled by the belief that through quantifying every single aspect of their lives, humans can better understand themselves and the world, thus they can transform and improve.

loHO's project Biological Labour explores a scenario in which the possibility of transformation and improvement is curtailed, and humans' biological condition sets the limits of what is possible. Data Production Labour explores humans' quest for self-improvement through quantification technologies, revealing how in this process their production of data is exploited by different actors for economic, political and military purposes.

The contemporary quantified condition enforces a state in which humans believe it is possible to achieve endless improvement, change, progress and enhancement. Does this unlimited possibility provoke unlimited pressure in humans to constantly change, improve and upgrade their lives? Is social pressure systematized through quantification? Are specific parts of the social fabric more affected by this condition or does it affect humans regardless of their social class?

MICRO-TARGETING AND TACTICAL FICTION

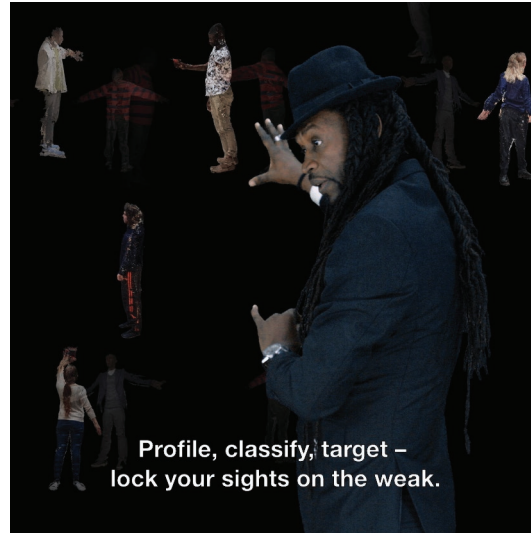
Date 1/2/2019 14:15 - 15:30

Organised by Privacy Salon

Location Area 42, Rue des Palais 46, 1030 Brussels

With Manu Luksch, Paul Bernal & TBC

Filmmaker, artist and researcher Manu Luksch (Open Society Fellow, Visiting Fellow Goldsmiths-University of London) will present her ongoing project Predictive City, which explores artistic strategies to demystify issues and engage the public in the



debate around algorithmic decision making.

Such systems promise general efficiency gains, significant advances in specific fields (such as medical image analysis), and protection against blatant human errors and biases. Predictive analytics and modelling raise the stakes not only for individuals, but also for entire societies. How might micro-targeted marketing or big data-driven predictions of behavior and morbidity impact the shape and possibilities of a person's life? ('We are serious. This is the end of dating'. eharmony). A proper understanding of what exactly is at stake is hampered by the forbidding difficulty of unpicking these technologies and the (often extravagant) claims made about them ('Solving Intelligence').

Luksch's project includes tools such as a browser plugin to highlight and interrogate key words associated with the algorithmic turn, an investigative film shoot inside one of the tech industry's leading player in smart city technologies, and media-process works such as ALGO-RHYTHM, which evokes the spectre of algorithmic electioneering.

COMPUTERS, PRIVACY & DATA PROTECTION

THANK YOU

This conference would not be possible without the industrious support of Sophie Vanaelst, 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, Tristan Bourbouze and Camille Charleux 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 Karin Neukermans for her great work behind the scenes doing the financial administration, Camille Van Puymbroeck for her wonderful communication and PR Support and 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 gratitude goes to Eike Gräf who kept on following up panels while he was already in a new 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 fantastic artistic programme and Pecha Kucha. Imge Ozcan, Kirsten Fiedler, Andreea Belu and Rocco Bellanova for organising a brilliant line-up for Privacy Camp. Alok Nandi (Architempo) for organising yet another fantastic Pecha Kucha! Many thanks to Pinelopi Troullinou, Mathieu D'Aquin and Ilaria Tiddi for organizing the Black Mirror Workshop this year at CPDP! Big thank you to Adam Harvey who designed this year's programme brochure cover.

Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth and Paul De Hert, the editors of the conference proceedings 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 CPDP2019 call for papers: Jef Ausloos, Emre Bayamlıoglu, Gergely Biczók, Michael Birnhack, Franziska Boehm, Edoardo Celeste, Damian Clifford, Colette Cuijpers, Lorenzo Dalla Corte, Silvia De Conca, Aviva de Groot, Massimo Durante, Michael Friedewald, Raphaël Gellert, Inge Graef, Dara Hallinan, Marit Hansen, Jaap-Henk Hoepman, Kristina Irion, Shaz Jameson, Lina Jasmontaite, Irene Kamara, Ioulia Konstantinou, Bert-Jaap Koops, Eleni Kosta, Tetyana Krupiy, Daniel Le Métayer, Alessandro Mantelero, Christopher Millard, Hiroshi Miyashita, Carolin Moeller, Nora Ni Loideain, Robin Pierce, Maria Grazia Porcedda, Claudia Quelle, Gianluigi Riva, Arnold Roosendaal, Joseph Savirimuthu, Iraklis Symeonidis, Ivan Szekely, Linnet Taylor, Omer Tene, Tjerk Timan, Rosamunde Van Brakel, Bart Van der Sloot, Yung Shin Van Der Syde, Joris van Hoboken, Sascha Van Schendel, Michael Veale, Gabriela Zafir-Fortuna, Nicolo Zingales, Frederik Zuiderveen Borgesius and for the CPDP2018 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, Lilian Edwards, Michael Friedewald, Lothar Fritsch, Raphaël Gellert, Gloria Gonzalez 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 CPDP2019 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 CPDP2019 would not have been possible!

DATA PROTECTION AND DEMOCRACY