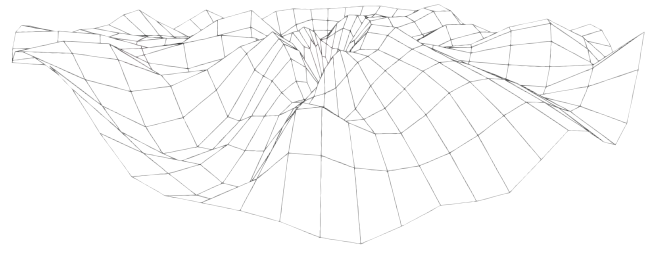
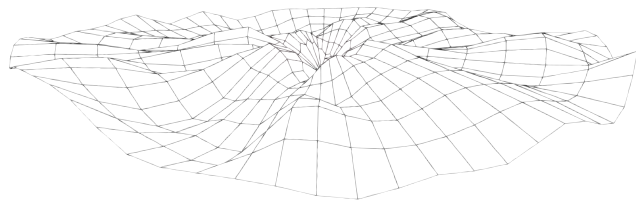


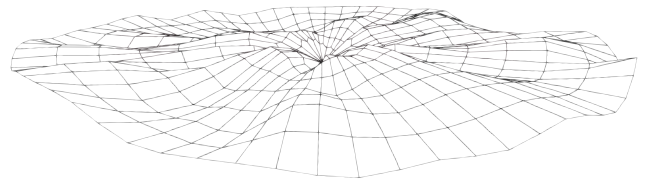
I'm



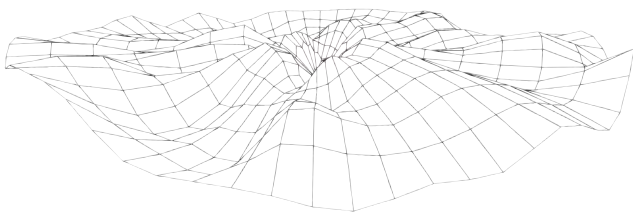
S



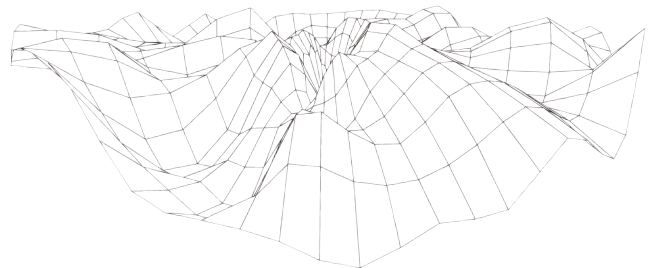
O



R



R



Y

15th INTERNATIONAL CONFERENCE 📅 23 - 25 MAY 2022 📍 BRUSSELS, BELGIUM
COMPUTERS, PRIVACY & DATA PROTECTION
#CPDP | DATA PROTECTION & PRIVACY
2022 | IN TRANSITIONAL TIMES

15th INTERNATIONAL CONFERENCE
23 - 25 MAY 2022 • BRUSSELS, BELGIUM
COMPUTERS, PRIVACY
& DATA PROTECTION
CPDP2022
DATA PROTECTION
& PRIVACY IN
TRANSITIONAL
TIMES



Cover Art © Artist: Taietzel Ticalos, screen shots from the video 'Shapes of Regret' when Yahoo! CEO apologizes for a data breach (2018 - 2022)

Pick the Right Footwear.

It is hard to write a foreword when the ground is not stable. Things (CPDP included) move, and the golden rule of hiking applies more than ever: *Pick the Right Footwear*. We recommend lightweight hiking boots as opposed to heavier or lighter footwear: some trails might be rocky, others might be easier to walk on, but it is hard to anticipate, so keep options open.

At the programming site of CPDP we faced similar hard choices. Aiming at breaking news-oriented panels is one of our ambitions, but the news that breaks changes daily. At the technology front there are reported breakthroughs about super and quantum computers. Some of the new computation miracles are now produced in Asia, yet another breakthrough in terms of the geopolitics of innovation.

At the regulatory front Europe, and the European Union, is still leading in many respects, and, to believe the *Washington Post* (April 22, 2022), its laws now are expected to influence the regulatory debate in the United States. We at CPDP believe that the influence will not be straightforward and that a 'gold standard for regulating online platforms' has not been reached. First Amendment concerns might explain for more political insistence in the States on a more hands-off approach to content moderation, to give just one example. Rather than propagating a regulatory race, CPDP stands for propagating discussions internationally, whereby concerns and experiences ('what works?') are compared and assessed. Leading EU Commissioner Margrethe Vestager's tweet for example ("The Digital Services Act will make sure that what is illegal offline is also seen & dealt with as illegal online — not as a slogan, as reality! And always protecting freedom of expression!") will be one of the references in the debate. At face value, the tweet seems to promise the best of all possible worlds in hardly fair terms, since what is bothering the political elite in Europe is not so much illegal information on social media, but some legal information that is considered 'harmful'.

"Free speech is the bedrock of a functioning democracy, and Twitter is the digital town square where matters vital to the future of humanity are debated," Musk said in a statement at end of April after having put \$44 billion on the table to buy Twitter. The agency of big firms in the realm of human rights is a classical topic of attention at CPDP, and many voices, including academics, feel strongly about this topic. Equally, in April 2022, Google, after having been alerted by the scientific community, banned dozens of apps from its Google Play store for using hidden data-harvesting software that documents link to U.S. national-security contractors. Creating a safe infrastructure for our digital society cannot be entrusted only to governments.

Speaking of which. The past year has further obscured our understanding of good and bad, when *The New Yorker* ('How democracies spy on their citizens') revealed another spy scandal, this time by the Spanish government, making use of the controversial spy technology *Pegasus*.

It is common to hear that the many seemingly unprecedented events and developments that characterized the experience of 2020 and 2021, have contributed to the feeling that we are living in a time of transition and change — both for better and for worse. CPDP in May (as opposed to CPDP in January) will (hopefully) be one without quarantine measures and travel restrictions and allow for networking and drinks after intensive days listening and debating. We learned from the 'digital' restructuring of the recent past. In particular *CPDP Global*, our new, online addition to this year's programme, must be mentioned in this respect. It spotlights global developments in data protection and privacy. This online track is screened for the CPDP in-person audience at La Cave, where the online and offline audiences are able to interact. The programme is bursting with activities. Join us, pick the right footwear, and travel light by leaving your dinner bowl at home to eat directly from the CPDP cook pot.

Warm Regards,

Paul De Hert

GENERAL CONGRESS INFORMATION

REGISTRATION & NAME BADGE

Registration opens on Sunday 22 May from 16:00 in La Cave at Les Halles. From Monday 23 to Wednesday 25 May, registration is in La Cave from 7:30. You will receive a name badge with the dates of attendance.

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 of Les Halles.

INTERNET LOGIN AND PASSWORD

Select SSID or Network: CPDP • Password: CPDP2022

VENUES

CPDP takes place simultaneously in two venues. Three tracks of sessions will take place at Area 42 - in the Grand, Midi and Petit rooms. Area 42 is located at 3 minutes walking distance (250 m) from Les Halles. Two tracks of sessions will take place at Les Halles - in the Grande Halle and La Cave. Maps will be available at the information desk in La Ruelle. There will be signposts and volunteers will help to show the way to Area 42.

LUNCH AND COFFEE BREAKS

Early lunch will start at 12:30 in Area 42. Regular lunch will start at 13:00 in Les Halles. To make the best of CPDP in spring-time, you can also take your lunch outside to the garden of Maison des Arts. Follow the signposts to find the garden (access via Les Halles). Coffee will be served in Area 42 and Les Halles.

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). Please switch off your phone during all sessions.

NETWORKING AND SIDE EVENTS

Cocktails will take place in Le Village starting at 18:30 on Monday and Tuesday and at 19:00 on Wednesday. Don't forget to follow the side events programme for more networking, receptions, and the official party in Area 42.

You can purchase drinks tokens from the registration desk in La Cave and the information desk in Area 42.

PLEASE RESPECT SILENT TIMES & AREAS

During the sessions, Le Village is closed (silent room!). The bars in La Ruelle and in Area 42 stay open for drinks (cash bar). Please switch off your phone during all sessions.

VIDEO RECORDING AND PHOTOPGRAPHY AT CPDP 2022

Is CPDP watching you? Well...a bit. A professional photographer will be taking photos at the conference venues, including crowd shots, which will then be used for publicity. Please let us know during registration if you do not wish to be in these photographs. All panels will be filmed at the Conference venue and uploaded to the archive after the event.

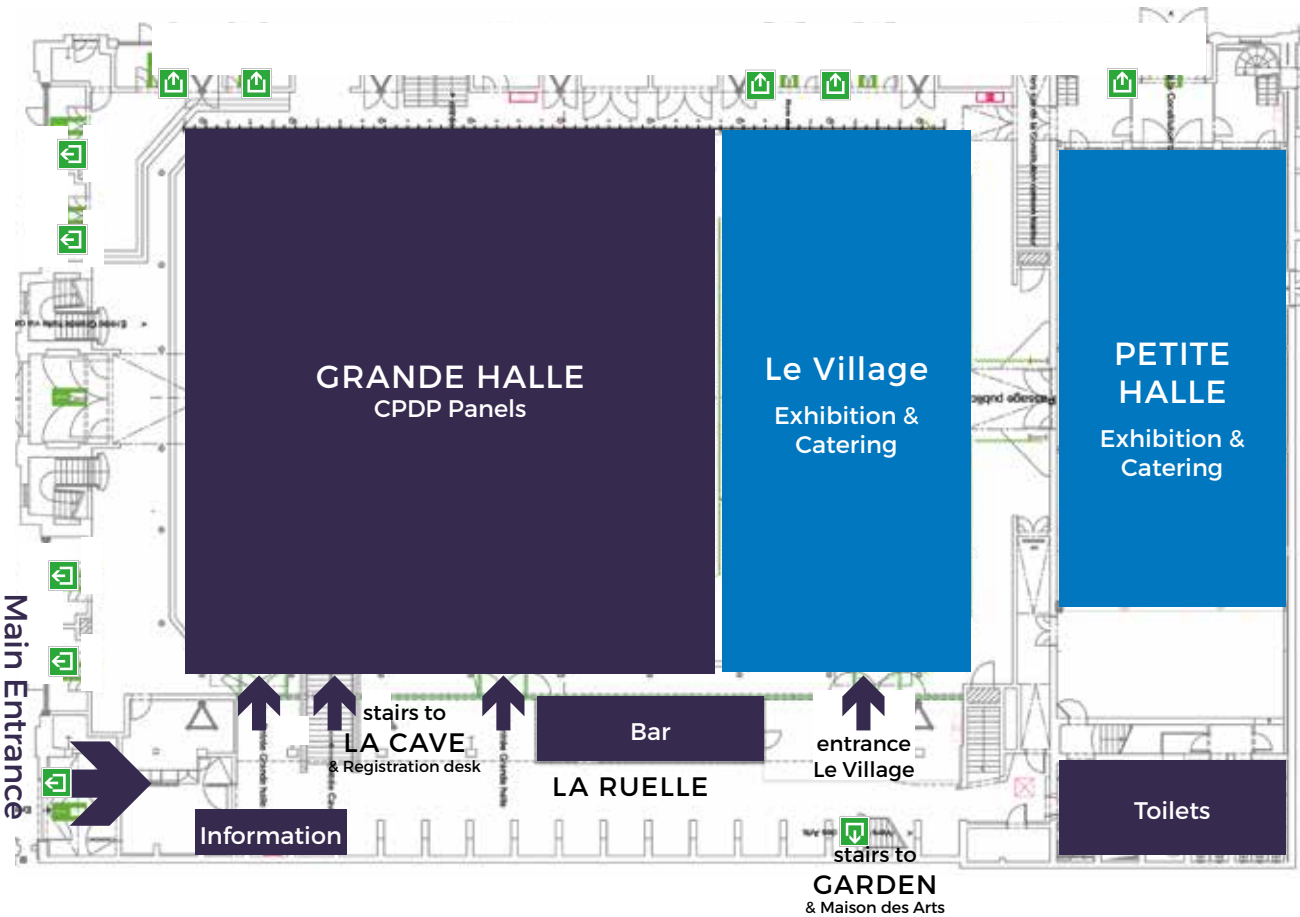
TAXI

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

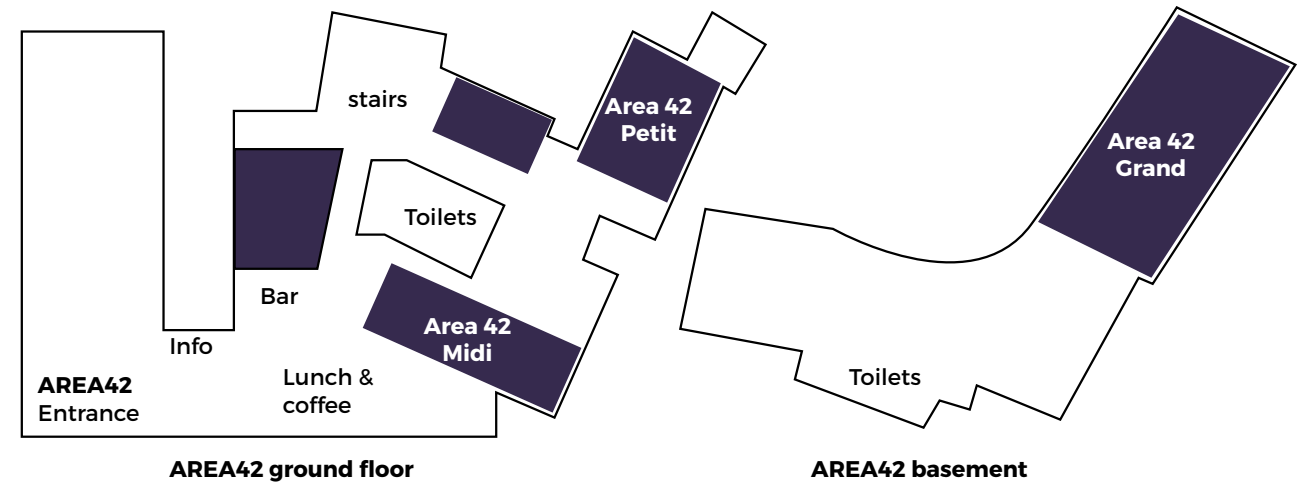
Please keep a close eye on email updates from us throughout the conference and contact the registration and information desks if you have questions. Our wonderful volunteers will also be at both venues to help find your way around the venues.

LES HALLES



Les Halles, Rue Royale-Sainte-Marie 22, 1030 Brussels (www.halles.be)

AREA 42



Area 42, Rue des Palais 46, 1030 Brussels (a 3-minute walk from les Halles de Schaerbeek)



RESTAURANTS

- Brasserie De Groene Ezel / L'âne Vert** (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

CPDP CONFERENCE BOOKS

Books based on papers presented at previous CPDP conferences:

- Dara Hallinan, Ronald Leenes, Paul de Hert, **Data Protection and Privacy, Volume 14, Enforcing Rights in a Changing World**, Oxford: Hart Publishing, 2021. (<https://www.bloomsbury.com/uk/data-protection-and-privacy-volume-14-9781509954513/>)
- Dara Hallinan, Ronald Leenes, Paul de Hert, **Data Protection and Privacy, Vol. 13, Data Protection and Artificial Intelligence**, Oxford: Hart Publishing, 2021. (<https://www.bloomsbury.com/uk/data-protection-and-privacy-volume-13-9781509941759/>)
- Dara Hallinan, Ronald Leenes, Serge Gutwirth, Paul De Hert, **Data Protection and Privacy, Vol. 12, Data Protection and Democracy**, Oxford : Hart Publishing, 2020. (<https://www.bloomsbury.com/uk/data-protection-and-privacy-volume-12-9781509953530/>)
- 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.bloomsbury.com/uk/data-protection-and-privacy-volume-11-9781509926206/>)
- Leenes, R., Van Brakel, R., Gutwirth, S. and P. De Hert, **Data Protection and Privacy: Vol. 10, The Age of Intelligent Machines**, Oxford: Hart Publishing, 2017 (<https://www.bloomsbury.com/uk/data-protection-and-privacy-volume-10-9781509919345/>)
- 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>)
- Gutwirth, S., Leenes, R. and P. De Hert, **Data Protection on the Move**, Dordrecht: Springer, 2016 (www.springer.com/gp/book/9789401773751)
- 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, **Reloading Data Protection**, Dordrecht: Springer, 2014. (www.springer.com/law/international/book/978-94-007-7539-8)
- Gutwirth, S., Leenes, R., De Hert, P. and Y. Poulet, **European Data Protection: Coming of Age** Dordrecht: Springer, 2012. (www.springer.com/law/international/book/9-)
- Gutwirth, S., Leenes, R., De Hert, P. and Y. Poulet, **European Data Protection: In Good Health?** Dordrecht: Springer, 2012. (www.springer.com/law/international/book/978-94-007-2902-5)
- Gutwirth, S., Poulet, Y., De Hert, P. and R. Leenes eds. **Computers, Privacy and Data Protection: an Element of Choice**. Dordrecht: Springer, 2011. (www.springer.com/law/international/book/978-94-007-0640-8)
- Gutwirth, S., Poulet, Y., and P. De Hert, eds. **Data Protection in a Profiled World**. Dordrecht: Springer, 2010. (www.springer.com/law/international/book/978-90-481-8864-2)
- Gutwirth, S., Poulet, Y., De Hert, P., de Terwangne, C., and S. Nouwt, eds. **Reinventing Data Protection?** Dordrecht: Springer, 2009. (www.springer.com/law/international/book/978-1-4020-9497-2)

RESTAURANTS

- Les Dames Tartine**
(Old-Fashioned luxury) €€€
Chaussée de Haecht 58,
1210 Brussels
+32 (0)2 218 45 49
Open: lunch and supper
- Café Bota**
(inside Le Botanique) (Italian) €€
Rue Royale 236, 1210 Brussels
+32 (0)2 226 12 28
Open: 12-14.30 and 18.30-23.00

Organisation of CPDP2022

DIRECTORS

- Paul De Hert (Vrije Universiteit Brussel LSTS, Tilburg University TILT), Director and Founder
- Bianca-Ioana Marcu (Vrije Universiteit Brussel, LSTS), Managing Director
- Dara Hallinan (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure), Programme Director
- Thierry Vandenbussche (Privacy Salon), Arts and Events Director

CORE PROGRAMMING COMMITTEE

- Paul De Hert (Vrije Universiteit Brussel LSTS, Tilburg University TILT)
- Bianca-Ioana Marcu (Vrije Universiteit Brussel LSTS)
- Dara Hallinan (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- Diana Dimitrova (FIZ Karlsruhe – Leibniz Institute for Information Infrastructure)
- Ana-Maria Hriscu (Tilburg University TILT)
- Bram Visser (Vrije Universiteit Brussel LSTS)

EXTENDED PROGRAMMING COMMITTEE

- Luca Belli (Fundação Getulio Vargas Law School)
- Dennis Hirsch (Ohio State University Moritz College of Law)
- Malavika Jayaram (Digital Asia Hub)
- Ronald Leenes (Tilburg University TILT)
- Omer Tene (International Association of Privacy Professionals)

PANEL COORDINATORS

- Maria Magierska (European University Institute)
- Lucas Van Wichelen (Vrije Universiteit Brussel)
- Guillermo Lazcoz (University of the Basque Country)
- Stephanie Garaglia (Vrije Universiteit Brussel, SCRI)
- Seyedeh Sajedeh Salehi (Vrije Universiteit Brussel, LSTS)
- Achim Klabunde (Computer scientist, data protection expert, former EU official)
- Ana Fernandez Inguanzo (Vrije Universiteit Brussel, LSTS)
- Bram Visser (Vrije Universiteit Brussel, LSTS)
- Hripsime Asatryan (Vrije Universiteit Brussel, LSTS)
- Javier López-Guzmán (Vrije Universiteit Brussel, LSTS)
- Nikolaos Ioannidis (Vrije Universiteit Brussel, LSTS)
- Katerina Demetzou (Radboud University)
- Alessandra Calvi (Vrije Universiteit Brussel, LSTS)
- Andrés Chomczyk Penedo (Vrije Universiteit Brussel, LSTS)
- Lander Govaerts (Vrije Universiteit Brussel, Chair in Surveillance Studies)
- Cristina Cocito (Vrije Universiteit Brussel, FRC)
- Olga Gkotsopolou (Vrije Universiteit Brussel, LSTS)

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, Ghent University (BE)
- Claudia Diaz, Katholieke Universiteit Leuven (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, Radboud 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, Institute for Information Law (IViR), University of Amsterdam (NL)
- Els Kindt, KU Leuven - CiTiP (BE), Universiteit Leiden - eLaw (NL) & EAB (European Association for Biometrics)
- Eleni Kosta, Tilburg Institute for Law, Technology and Society TILT (NL)
- Ronald Leenes, Tilburg Institute for Law, Technology and Society TILT (NL)
- Dave Lewis, ADAPT Centre (IE)
- Eva Lievens, Ghent University (BE)
- Jo Pierson, VUB-SMIT (BE)
- José-Luis Piñar, Universidad CEU-San Pablo (ES)
- Charles Raab, University of Edinburgh (UK)
- Marc Rotenberg, EPIC (US)
- Ivan Szekely, Central European University (HU)
- Frederik Zuiderveen Borgesius, iHub & iCIS Institute for Computing and Information Sciences, Radboud University Nijmegen (NL)

LOGISTICS AND REGISTRATION

medicongress
conference & association management

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

PRIVACY  **SALON**

Bianca-Ioana Marcu, Thierry Vandenbussche, Dara Hallinan, Karin Neukermans, Diana Dimitrova,
Justien Van Strydonck, Bram Visser, Ana Gagua, Tabea Wagner, Laura Bauer, Annette Monheim
www.privacysalon.org

Design © Nick Van Hee – www.nickvanhee.be

MONDAY 23RD MAY 2022

23.5	GRANDE HALLE	LA CAVE
7.30	Registration in La Cave	Registration in La Cave
8.30	Welcome and Introduction by Paul De Hert	Welcome and Introduction in Grande Halle
8.45	The Future of Global Data Flows organised by International Association of Privacy Professionals (IAPP) Page 16	How to Reconcile Facial Recognition Technologies with Consumers' Privacy organised by International Enforcement Working Group – Office of the Privacy Commissioner of Canada (CA) Page 18
10.00	Coffee break	Coffee break
10.30	The Future at the Intersection of Knowledge Creation, Research, and Individual Sovereignty organised by Interpublic Group Page 16	Genetic Data: a Challenge for the EU Data Protection Framework? organised by PANELFIT (UPV/EHU) Page 19
11.45	Are Democratic Institutions Doing Enough to Protect Democracy, Freedom and Privacy from the Threat of Monopoly Power? organised by Open Markets Institute Page 17	Future of AI Policy organised by Center for AI and Digital Policy Page 19
13.00	Lunch	Lunch
14.15	The AI Act: Where Are We, and Where Are We Going? organised by CPDP Introductory Speech by European Commissioner for Justice, Didier Reynders Page 17	Data Protection Engineering: What Is the Road Ahead? organised by European Union Agency for Cybersecurity (ENISA) Page 20
15.30	Coffee break	Coffee break
16.00	Calibrating the AI Act – Is It the Right Framing to Protect Personal and Fundamental Rights? organised by Microsoft Page 18	<i>Schrems II</i> : 18 months later: much ado about nothing or a game changer? organised by EDPS Page 20
17.15	Regulation of Global Data Flows: a Story of the Impossible? organised by EDPS Page 18	Digital Platforms, the New Privacy Champions? Between Myths and Realities organised by Computer Law and Security Review Page 21
18.30	Cocktail sponsored by EDPS in Le Village	

AREA 42 GRAND	AREA 42 MIDI	AREA 42 PETIT
Registration in La Cave	Registration in La Cave	Registration in La Cave
Welcome and Introduction in Grande Halle	Welcome and Introduction in Grande Halle	Welcome and Introduction in Grande Halle
Data Protection as Corporate Social Responsibility organised by European Centre on Privacy and Cybersecurity (ECPC), Maastricht University Page 21	Data Protection Regulation Post-COVID: the Current Landscape of Discussions in Europe, the US, India and Brazil organised by Data Privacy Brasil Research Association Page 24	Protecting the Rights and Ensuring the Future of Generation AI organised by AI4Belgium Page 27
Coffee break	Coffee break	Coffee break
Governance and Regulation of AI from the Perspective of Autonomy and Privacy organised by Campus Fryslân - Data Research Centre (DRC) Page 22	DPAs in the COVID-19 Pandemic organised by CPDP Page 24	Regulating AI in Health Research and Innovation organised by Department of Innovation and Digitalisation in Law, University of Vienna Page 27
Assessing the Impact on Fundamental Rights in AI Applications organised by Politecnico di Torino Page 22	Data Protection Concerns in the AML/CFT Framework organised by Tilburg Institute for Law, Technology, and Society and Digital Legal Studies Page 25	A Sand Storm or Just a Breeze? What's the Fuss About Sand-boxes? organised by Norwegian Data Protection Authority Page 28
Lunch	Lunch	Lunch
EU Cloud Code of Conduct: 1 Year Anniversary - Operationalising GDPR Compliance organised by Workday Page 22	Secondary Use of Personal Data for (Biomedical) Research organised by CiTiP, KU Leuven Page 25	The Return of Privacy? 'Smart Video Surveillance' Evaluating Data Protection in the Light of Privacy and Surveillance organised by VUB Chair in Surveillance Studies Page 28
Coffee break	Coffee break	Coffee break
GDPR Certification Schemes: General vs. Specific Schemes – What Do Effective Schemes Look Like? organised by Alexander von Humboldt Institute for Internet and Society Page 23	Sharing the Digital Me – a Contextual Integrity Approach for Discussing Governance of Health and Genetic Data in Cyberspace organised by Uppsala University Page 26	Encoding Identities: the Case of Commercial DNA Databases organised by University of Amsterdam Page 29
The AI Act and the Context of Employment organised by European Trade Union Institute Page 23	Manipulative Design Practices Online: Policy Solutions for the EU and the US organised by TACD and Norway Consumer Council Page 26	Effective Transparency and Control Measures (Including Privacy Icons): the Example of Cookie Banners. Where Do We Stand Now? organised by Berlin University of the Arts Page 29
Cocktail sponsored by EDPS in Le Village		

24.5 GRANDE HALLE		LA CAVE [CPDP Global]
7.30	Registration in La Cave	<h2>CPDP Global</h2> <p>CPDP Global panels ongoing. Head to pages 33-37 for full line-up.</p>
8.45	Convergence in Action: Regional and Global Cooperation Between Data Protection Authorities organised by European Commission Page 30	
10.00	Coffee break	Coffee break
10.30	Global Governance of Privacy: Beyond Regulation organised by Apple Page 30	Smart Borders? Artificial Intelligence at the EU Border organised by Karlsruhe Institute of Technology Page 34
11.45	Leveraging AI: Risks & Innovation in Content Moderation by Social Media Platforms organised by Meta Page 31	Privacy Preserving Advertising: Prospects and Paradigms organised by Mozilla Page 34
13.00	Lunch	Lunch
14.15	Re-framing Data Use: Values, Norms, Institutions organised by The Ditchley Foundation Page 31	<h2>CPDP Global</h2> <p>CPDP Global is a new, online addition to this year's programme, spotlighting global developments in data protection and privacy. The online track is screened for the CPDP in-person audience at La Cave, where the on-line and offline audiences are able to interact. Head to pages 33-37 for the full line-up of CPDP Global panels, running from 7:30 till 21:15.</p>
15.30	CNIL-Inria Privacy Award, EPIC Champion of Freedom Award	
16.00	Innovation in Cybersecurity - Accelerating Europe's Digital Transformation and Digital Resilience Through Stronger Partnerships organised by Google Page 32	
17.15	Data Protection and High-tech Law Enforcement – the Role of the Law Enforcement Directive organised by EU Agency for Fundamental Rights (FRA) Page 32	
18.30	Cocktail sponsored by EPIC in Le Village	

AREA 42 GRAND	AREA 42 MIDI	AREA 42 PETIT
Registration in La Cave	Registration in La Cave	Registration in La Cave
See You in Court! – Discussing the Potential and Challenges of Judicial Actions for GDPR Infringements organised by LSTS and ALTEP DP Page 37	UPLOAD_ERROR: Automated Decisions, Users' Right to Redress, and Access to Justice on Social Networks organised by Amsterdam Law & Technology Institute, VU Amsterdam Page 40	GoodBrother: Privacy, Corona-Virus, and Assisted Living Technologies organised by Cost Action 19121 'GoodBrother' Page 43
Coffee break	Coffee break	Coffee break
Concrete and Workable Solutions to the GDPR Enforcement organised by NOYB Page 37	Closed Session organised by CPDP	Responsible IoT in Public Space - Who is Actually Responsible for What? organised by University of Twente / Project BRIDE Page 43
Interdisciplinary Data Protection Enforcement in the Digital Economy organised by European Consumer Organisation (BEUC) Page 38	Police: We Can't Stand Losing You - Fortnite Undercover Avatars Are Only the Beginning organised by EDEN Page 40	Big Brother Out to Lunch organised by PROTEIN, H2020 project Page 44
Lunch	Lunch	Lunch
Collectively Making It Work: (F)Laws of Individual Approaches to Resist Platform Power organised by IViR, University of Amsterdam Page 38	Research and Best Practice to Address Socio-technical Risks in AI Systems organised by Microsoft Page 41	Privacy Design, Dark Patterns, and Speculative Data Futures organised by SnT, University of Luxembourg Page 44
Coffee break	Coffee break	Coffee break
Dark Patterns and Data-Driven Manipulation organised by Leiden University Page 39	Data Protection Certification – International Perspective and Impact organised by Mandat International, International Cooperation Foundation Page 41	EDPL Young Scholar Award organised by EDPL Page 45
Mobility Data for the Common Good? On the EU Mobility Data Space and the Data Act organised by Future of Privacy Forum Page 39	Data Protection as Privilege? Digitalisation, Vulnerability and Data Subject Rights organised by SPECTRE project Page 42	Technology and Power in Times of Crisis organised by Global Data Justice project, Tilburg University Page 45
Cocktail sponsored by EPIC in Le Village		

WEDNESDAY 25TH MAY 2022

25.5	GRANDE HALLE	LA CAVE
7.30	Registration in La Cave	Registration in La Cave
8.45	Can Law Be Determinate in an Indeterminate World? organised by CDSL Page 46	Personal Data in Texts: Detection, Annotation and Governance organised by Université de Bourgogne Franche-Comté (UBFC) Page 48
10.00	Coffee break	Coffee break
10.30	Practical Legal Perspectives on International Transfers organised by CPDP Page 46	Digital Age of Consent: Looking for a New Paradigm organised by CEU San Pablo University - South EU Google Data Governance Chair Page 49
11.45	International Transfers on the Ground organised by CPDP Page 47	Transitional (Legal) Times for R&D and R&I Sectors organised by VALKYRIES H2020 Project - LIDER Lab Scuola Sant'Anna - Ethical Legal Unit Page 49
13.00	Lunch	Lunch
14.15	Will the Digital Ever Be Non-binary? The Future of Trans (Data) Rights organised by CPDP Page 47	Role of Ethics Committees in the European Health Data Space organised by CPME – Standing Committee of European Doctors Page 50
15.30	Coffee break	Coffee break
16.00	Trust & Transparency in AI: Discussing How to Unpack the “Black Box” organised by Uber Page 47	Data Protection New Frontiers in BRICS Countries organised by Center for Technology and Society at FGV / CyberBRICS Project Page 50
17.15	Why Privacy Matters and the Future of Data Protection Law organised by Cordell Institute, Washington University Page 48	Synthetic Data Meet the GDPR: Opportunities and Challenges for Scientific Research and AI organised by University of Turin / UNITO Page 51
18.30	Closing Remarks by Paul De Hert and Wojciech Wiewiórowski (EDPS)	Closing Remarks in Grande Halle
19.00	Cocktail sponsored by Privacy Salon in Le Village	

AREA 42 GRAND	AREA 42 MIDI	AREA 42 PETIT
Registration in La Cave	Registration in La Cave	Registration in La Cave
From Shareholder Value to Social Value organised by IEEE Page 51	PIMS Building the Next Generation Personal Data Platforms, A Human-Centric Approach organised by Internet Users Association Page 54	A Cybersecurity Incident: Who You Gonna Call? organised by Université du Luxembourg Page 57
Coffee break	Coffee break	Coffee break
Tackling Surveillance and Its Business Model Through Decentralisation - Discussing Infrastructure and Token Economics organised by Nym Technologies Page 52	Measuring Fundamental Rights Compliance Through Criminal Justice Statistics organised by MATIS project Page 55	Academic Session 1 organised by CPDP Page 57
Power over Data and Algorithms: Can We Get it Back? organised by Ada Lovelace Institute Page 52	Book Session: ‘Industry Unbound’ by Ari Waldman organised by CPDP and the Chair ‘Fundamental Rights and the Digital Transformation’ at VUB Page 55	Academic Session 2 organised by CPDP Page 58
Lunch	Lunch	Lunch
Is a European Data Strategy Without Trade-offs Between Economic Efficiency and Fundamental Rights Protection Possible? organised by Open Future Foundation Page 53	False Privacy in Sheep’s Clothing: Harmful Patterns in Recent “Privacy” Proposals organised by Brave Page 56	Limiting State Surveillance by Means of Constitutional Law: Potentials and Limitations organised by Fraunhofer ISI Page 58
Coffee break	Coffee break	Coffee break
Limits of Emergency Powers: Protecting Privacy in Exceptional Circumstances organised by EPIC Page 53	Justice 3.0: AI In and For Justice and Case-law as Big Data Challenges organised by Scuola Superiore Sant’Anna Page 56	Academic Session 3 organised by CPDP Page 59
When Privacy and Data Protection Rules, What and Who Loses Out? organised by Interdisciplinary Hub for Digitisation and Society, Radboud University Nijmegen Page 54	Empowering the AI Act: Limits and Opportunities organised by Smart Global Governance / EDHEC Augmented Law Institute Page 56	Government Access to Data Held by the Private Sector: How Can Democracies Show the Way? organised by Georgia Institute of Technology, School of Cybersecurity and Privacy Page 59
Closing Remarks in Grande Halle	Closing Remarks in Grande Halle	Closing Remarks in Grande Halle
Cocktail sponsored by Privacy Salon in Le Village		

MONDAY 23RD MAY 2022

07:30 - Registration in La Cave
08.15 - Welcome coffee in Le Village

CPDP2022 PANELS AT GRANDE HALLE

08:30 - WELCOME AND INTRODUCTION BY PAUL DE HERT IN GRANDE HALLE

08:45 – THE FUTURE OF GLOBAL DATA FLOWS

Business☆☆☆ **Policy**☆☆☆

Organised by International Association of Privacy Professionals (IAPP)

Moderator Caitlin Fennessy, IAPP (US)

Speakers Hiroshi Miyashita, Chuo University (JP); Ralf Sauer, European Commission (EU); Joe Jones, UK Department for Digital, Culture, Media and Sport (UK); Katherine Harman-Stokes, U.S. Department of Justice (US)

In recent years, data protection laws have proliferated across the globe. While many of these laws take inspiration from the GDPR, each brings with it nuanced approaches to data protection and information transfer restrictions along with unique cultural norms and legal systems. China and Brazil have new data protection and transfer rules, India is soon to join them and the UK is considering modernizing its framework. Developing data transfer compliance programs has become organizations' top privacy challenge, kept outside counsel busy, and led policymakers to debate even the definition of data transfers themselves. Companies must adopt myriad country-specific transfer contracts to govern the crisscrossing data that fuels the global economy and informs our society. As data transfers transition from a transatlantic to a global challenge, is a more global approach possible?

- What will new global players in the field of data protection law mean for international transfers?
- How will the EU scale or shift its adequacy model?
- Will the US build on its APEC CBPR strategy as a potential multilateral alternative?
- Will the UK develop a meaningful new approach and what might that entail?

10:00 - COFFEE BREAK

10:30 – THE FUTURE AT THE INTERSECTION OF KNOWLEDGE CREATION, RESEARCH, AND INDIVIDUAL SOVEREIGNTY

Academic☆☆ **Business**☆☆☆ **Policy**☆☆☆

Organised by Interpublic Group

Moderator Alexander White, Privacy Commissioner of Bermuda (BM)

Speakers Sheila Colclasure, Interpublic Group (US); Brendan Van Alsenoy, European Data Protection Supervisor (EU); Hattie Davison, UK Department of Culture, Media, and Sport (UK); Martin Abrams, Duke University (US); Chris Foreman, Merck Sharp & Dohme (US)

The resolution of friction between personal sovereignty and the shared fruits of scientific and private research are a necessity as society accelerates into the digital age, one where observational technology enables connected marketplace, commerce, and government. This future will be heavily reliant on the utility of technology that observes and technology that algorithmically processes data that relates to people, things, and places, both for insight (knowledge discovery) and research (academic and commercial) and then make decisions lawfully based on that knowledge. This friction is very much in play in numerous legislative and regulatory proceedings. It has been exacerbated by the acceleration of observational technology. This session will discuss more nuanced approaches to fair governance of advanced analytics in an observational age.

- In an observational age, driven by algorithms, are there quick answers to what is framed as “surveillance capitalism”?
- Is a more nuanced approach that finds the equilibrium between knowledge discovery and individual sovereignty possible?

- Do we need a regulatory approach that measures risk based on the individual impactfulness of research and knowledge creation, versus the risks associated with decisions and actions?
- Does fairness require approaches that more evenly balance the full range of fundamental rights that come into play with knowledge creation?

11:45 – ARE DEMOCRATIC INSTITUTIONS DOING ENOUGH TO PROTECT DEMOCRACY, FREEDOM AND PRIVACY FROM THE THREAT OF MONOPOLY POWER?

Academic☆☆ **Business**☆☆ **Policy**☆☆☆☆

Organised by Open Markets Institute

Moderator Christian D’Cunha, DG Connect (EU)

Speakers Cristina Caffarra, Charles River Associates (IT); Barry Lynn, Open Markets Institute (US); Johnny Ryan, Irish Council for Civil Liberties (IE); René Repasi, MEP (EU)

Recent years have seen an acceleration in moves to regulate big tech, through privacy and competition rules and other new tools like attempts to contain ‘illegal online content’. In the meantime, the biggest companies seem to get yet more powerful, with their business models barely affected. This discussion will explore how restrictions and costs of getting to court, as well as underlying growing inequality, are holding back fundamental rights, and what can be done about it.

- Of what value are all these laws when the worst offenders seem able to leverage their lobbying and litigation resources to act with impunity?
- How can citizens overcome rules on ‘standing’ to contest decisions like on mergers that seem threaten civil liberties, democracy and free markets with ‘death by a thousand cuts’?
- Are our analytical tools legalistic and outdated?
- What can a democracy do to ensure equality before the law in the face of big tech?

13:00 - LUNCH

14:15 – THE AI ACT: WHERE ARE WE, AND WHERE ARE WE GOING?

INTRODUCTORY SPEECH BY EUROPEAN COMMISSIONER FOR JUSTICE, DIDIER REYNDEERS

Academic☆☆ **Business**☆☆ **Policy**☆☆

Organised by CPDP

Moderator Omer Tene, Goodwin (US)

Speakers Gianclaudio Malgieri, EDHEC Business School (FR); Charles-Albert Helleputte, Steptoe (BE), Katarzyna Szymielewicz, EDRI (BE); Anna Moscibroda, DG Just (EU); Sylwia Giepmans-Stepien, Google (BE)

It seems there is currently no topic more discussed than AI. It also seems there is no EU legislative proposal more discussed than the AI Act. Since the initial proposal for the Act was released in the first half of 2021, countless articles, statements and opinions have been offered on its quality, prospects and likely impact. Some see the Act as offering a reasonable and balanced approach to a novel and uncertain technological development, others see that Act as flawed – for a number of different reasons. Against this background, this high-level panel brings together experts from a range of sectors, and with a range of perspectives, who will seek to explore the space of the AI Act and, in particular, will consider the following questions:

- What is the future of the AI Act, and on what timescale?
- What are the key problems with the Act, and how might they be resolved?
- How is the Act likely to change moving towards adoption, and what are the likely drivers of change?
- What will the impact of the Act be, in Europe, and elsewhere?

15:30 - COFFEE BREAK

16:00 – CALIBRATING THE AI ACT – IS IT THE RIGHT FRAMING TO PROTECT PERSONAL AND FUNDAMENTAL RIGHTS?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Microsoft
Moderator Jay Modrall, Norton Rose Fulbright LLP (BE)
Speakers Georg Borges, University Saarland (DE); Frederico Oliveira da Silva, BEUC - The European Consumer Organisation (EU); Alžbeta Krausová, Institute of State and Law of the Czech Academy of Sciences (CZ); Cornelia Kutterer, Microsoft (BE)

On 21 April 2021, the European Commission presented its proposal for a novel regulatory framework for AI. The proposal aims to chart the European path to trustworthy development and deployment of AI-driven products, services and systems. This panel will critically examine whether the foundation and structure of the AI Act - grounded in product safety legislation - can properly address risks to fundamental rights such as the right to human dignity, equality between women and men, freedom of assembly or the general principle of good administration.

- What is the rationale behind the AI Act’s product safety approach?
- What are the potential benefits and shortcomings of that approach?
- Are there learnings from other legal domains that could be helpful (such as tort law or data protection)?
- Does the approach accommodate the socio-technical challenges of AI systems?

17:15 – REGULATION OF GLOBAL DATA FLOWS: A STORY OF THE IMPOSSIBLE?

Business ☆ **Policy** ☆☆☆☆☆
Organised by EDPS
Moderator Wojciech Wiewiórowski, European Data Protection Supervisor (EU)
Speakers Ulrich Kelber, Federal Commissioner for Data Protection and Freedom of Information (DE); Audrey Plonk, OECD (INT); Vera Jourová, Vice President of the European Commission for Values and Transparency (EU); Ana Brian Nougères, United Nations (INT); Graham Greenleaf, UNSW (AU)

This high-level panel will discuss the future of international transfers regulation, including the issue of surveillance (aka “government access to data”) and the “data flows with trust” concept which appears to be gaining momentum since its introduction by Japan in the G7 context. Its objective would be to bring the EU data protection regulators’ perspective in relation to a debate which so far takes place mainly in other fora (OECD, CoE, bilateral EU-US discussions) and to explore possible long-term solutions that could satisfy the high standards of the EU Charter of Fundamental Rights and the CJEU case law.

- What is the current state of play of post-GDPR adequacy reviews? As adequacy decisions are a long and time-consuming process, what expectations for facilitating data flows between the EU and the rest of the world can they realistically fulfil?
- Is there an inherent contradiction between “data sovereignty” and data localisation and the “push for the free flow of data in the digital world”, both of which are simultaneously promoted by the EU in various contexts?
- What multilateral solutions could be envisaged and within what timeframe? What can we learn from other models of regulation of data flows?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2022 PANELS AT LA CAVE

08:45 – HOW TO RECONCILE FACIAL RECOGNITION TECHNOLOGIES WITH CONSUMERS’ PRIVACY

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by International Enforcement Working Group – Office of the Privacy Commissioner of Canada
Moderator Michael Maguire, Office of the Privacy Commissioner (CA)

Speakers James Dipple-Johnstone, UK Information Commissioner’s Office (UK); Daniel Leufer, Access Now (BE); Plamen Angelov, EDPS (EU); Quang-Minh Lepescheux, Microsoft (US); Joan S. Antokol, Park Legal LLC (US)

Owing to rapid technological innovations in biometric technology, including improvements to facial recognition (FRT) algorithms and the unprecedented availability of personal images, FRT is perceived as an easy and reliable biometric solution for identifying and authenticating individuals. The demand and temptation to deploy FRT solutions and services (hiring, policing, marketing, etc.) continues to grow all over the world, both in the private and public sectors. But, alas, every tech rose has its thorn and FRT is not an exception insofar as it constitutes a significant threat to individuals’ privacy if deployed outside legal parameters.

In this session, the panellists will outline the state of play in the world through concrete examples of national/regional strategies, recent investigations (including Clearview AI), and regulations and policy orientations in relation to private and public sector uses of FRT. The panel will consider:

- What are the different uses of FRT in the public and private sectors?
- What are the challenges to adapt certain PDP principles to FRT?
- How to reconcile the benefits of FRT and individuals’ privacy protection?
- What are the lessons learned from recent investigations on the use of FRT by private and public organisations?
- What are the different trends regarding regulating FRT?

10:00 - COFFEE BREAK

10:30 – GENETIC DATA: A CHALLENGE FOR THE EU DATA PROTECTION FRAMEWORK?

Academic ☆☆☆ **Policy** ☆☆☆
Organised by PANELFIT (UPV/EHU)
Moderator Regina Becker, University of Luxembourg (LU)
Speakers Lisa Diependaele, EU Commission (EU); Iñigo De Miguel, University of The Basque Country/Upv-Ehu (ES); Marta Tomassi, University of Trento (IT); Illaria Colussi, Bbmri-Eric (AT)

The EU data protection legal framework was built around the data subject. Normally, we assume that this is a single person. This is not always the case when we consider health data in general and genetic data in particular. As we all know, there are thousands of diseases that have a genetic component. This component is sometimes inheritable. This means that if we gain access to someone’s genetic information, we can also know, or at least suspect, what the genetic endowment of his or her relatives may be. This information is therefore very relevant for all those involved. However, the GDPR is mainly built on the perspective of the individual. This perspective does not work so well with the type of issues that genetic information raise. This panel is comprised to analyse such issues from a multidisciplinary point of view:

- Could we consider that genetic data are personal data of different data subjects (not only the one who provided the biological sample)?
- Should other people’s rights prevail against the sample donor’s will not to share the data in some concrete circumstances?
- Are physicians allowed to break confidentiality if circumstances recommend it?
- Does the fact that the sample donor is dead make any difference on this framework?

11:45 – FUTURE OF AI POLICY

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Center for AI and Digital Policy (US)
Moderator Merve Hickok, Alethicist.org (US)
Speakers Sarah Chander, EDRI (BE); Gregor Stojin, Committee on AI, Council of Europe (EU); Brando Benifei, European Parliament (EU); Doaa Abu-Elyounes, UNESCO Bioethics and Ethics of Science Section, Ecole Normale Supérieure ENS Paris (FR)

AI policy is moving forward quickly. More than 50 countries have endorsed the OECD AI Principles or the G20 AI Guidelines. 2021 saw the introduction of the EU AI Act, the adoption of UNESCO Recommendation on the Ethics of AI, and the Council of Europe’s outline for an international treaty on AI, based on human rights, democracy, and the rule of law. Also, the U.N. human rights chief called for a moratorium on the use of AI techniques that poses a risk to human rights or fails to comply

with international human rights laws. But key questions remain about the prospects for “red lines,” the implementation of policy commitments, and the ongoing problem of bias across AI. Panellists will discuss:

- Countries have agreed on the need to prohibit social scoring, but there is still no consensus on the need to prohibit facial surveillance. What steps are necessary to achieve that goal?
- How does endorsement of principles by countries compare to their practices?
- What are the prospects for the EU AI Act?
- Which key AI policy developments should we expect in 2022?

13:00 - LUNCH

14:15 – DATA PROTECTION ENGINEERING: WHAT IS THE ROAD AHEAD?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by European Union Agency for Cybersecurity (ENISA) (EU)

Moderator Prokopios Drogkaris, ENISA (EU)

Speakers Marit Hansen, Unabhängiges Landeszentrum für Datenschutz/ULD (DE); Armand Heslot, CNIL (FR); Kim Wuyts, KU Leuven, (BE); Gwendal Le Grand, European Data Protection Board EDPB (EU); Alex Li, Microsoft (US)

Data Protection Engineering, i.e., embedding data protection requirements into the information systems’ design and operation, has emerged over the last years, further to the legal obligation of data protection by design. Proper and timely inception, development and integration of technical and organizational measures into data processing activities play a big role in the practical implementation of different data protection principles. The aim of this panel will be to discuss the evolution of data protection engineering approaches, the current practices and discuss existing and emerging challenges.

- Has the evolution of technology and deployment models affected data protection engineering?
- How should data protection engineering be perceived within the context of emerging technologies?
- To what extent is it possible to create direct links between data protection engineering technologies and techniques and data protection principles?
- How can a data controller provide a certain level of assurance with regards to the data protection engineering approach followed?

15:30 - COFFEE BREAK

16:00 – SCHREMS II: 18 MONTHS LATER: MUCH ADO ABOUT NOTHING OR A GAME CHANGER?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by EDPS

Moderator Thomas Zerdick, EDPS (EU)

Speakers Magdalena Cordero, European Court of Auditors (EU); Raluca Peica, Curia (EU); Peter Parycek, Fraunhofer FOKUS Institute (DE); Jan Albrecht, Minister for Energy, Agriculture, the Environment, Nature and Digitalization of Schleswig-Holstein (DE)

This panel will consider how the Schrems II judgment so far impacted international transfers in practice and discuss ongoing initiatives such as the “European cloud”, Gaia-X, and legal and technical questions of data sovereignty and data localisation. It aims to provide an overview of relevant developments during the past year as well as important ongoing initiatives, including in the area of enforcement.

- How effective has the EU been so far in applying and enforcing the CJEU Schrems II judgment?
- What kind of technical and organisational measures have organisations put in place to apply the Schrems II judgment and to ensure an adequate level of protection?
- Could the adhesion of non-EU cloud operators to sovereign projects, such as Gaia-X or to the approved EU-wide cloud codes of conduct, solve the Schrems II challenge?
- How can organisations in the EU avoid non-EU government surveillance in practice and are there any lessons to be learned in this respect from the UK adequacy decisions?

17:15 – DIGITAL PLATFORMS, THE NEW PRIVACY CHAMPIONS? BETWEEN MYTHS AND REALITIES.

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by Computer Law and Security Review (UK)

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

Speakers Joris Van Hoboken, Vrije Universiteit Brussels (BE); Inge Graef, Tilburg University (NL); Olivier Blazy, Ecole Polytechnique (FR); Martin Bieri, CNIL (FR); Mehwish Ansari, Article 19 (US)

Digital platforms are now penetrating almost all aspects of our lives. After having built immense walled gardens without conceiving privacy as a core design value, they are now making bolder privacy claims and implementing privacy enhancing technologies (PETs) in different settings. By way of example, Google and Apple have been developing local differentially private techniques for services such as web browsing and maps or federated learning techniques to reduce the processing of behavioral data for marketing purposes. Google and Apple have also partnered to create an exposure notification system in service of privacy-preserving contact tracing. In this panel, CLSR brings together lawyers, computer scientists and regulators to discuss the benefits and limits of a value-by-design approach and its instrumentalization by digital platforms, which are primarily focused upon strengthening their market and information powers.

- Are digital platforms at the forefront of privacy innovation?
- What do these PETs really achieve?
- How do/could digital platforms use these PETs to strengthen their market position & information power?
- What is the role of a supervisory authority in this context and what could be done to counter-balance excessive centralization of power in the hands of digital platforms?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2022 PANELS AT AREA 42 GRAND

08:45 – DATA PROTECTION AS CORPORATE SOCIAL RESPONSIBILITY

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

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

Moderator Paolo Balboni, ECPC, Maastricht University (NL)

Speakers Sophie Nerbonne, CNIL (FR); Stefano Fratta, Meta (SP); Sarah Bakir, Rabobank (NL); Massimo Marelli, ICRC (INT); Cosimo Monda, ECPC, Maastricht University (NL)

In our data-centric global economy, businesses need to consider privacy and data protection as assets rather than simply compliance obligations. It has already been demonstrated that a strategic and accurate approach to data protection can generate a significant return on investment (ROI). With a research project currently running at ECPC Maastricht University, a group of academics, businesses and data protection- and intergovernmental stakeholders, studies ways to trigger virtuous data protection competition between companies by creating an environment that identifies and promotes data protection as an asset, which can be used to help companies to responsibly further their economic targets. This can be accomplished through the development of a new dimension of data protection that goes beyond legal compliance, transforming data protection into a new form of Corporate Social Responsibility (Data Protection as a Corporate Social Responsibility, DPCSR). Concrete, measurable and translatable guidance for organisations are being developed in order to answer the following questions, which will be discussed in the panel:

- What are the fundamental requirements of socially responsible data processing activities?
- How can companies reconstruct Data Protection into an effective CSR framework?
- What are the benefits for companies that embrace data protection as a CSR?

10:00 - COFFEE BREAK

10:30 – GOVERNANCE AND REGULATION OF AI FROM THE PERSPECTIVE OF AUTONOMY AND PRIVACY

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Campus Fryslân - Data Research Centre (DRC) (NL)

Moderator Andrej Zwitter, Campus Fryslân (NL)

Speakers Linnet Taylor, Tilburg Law School/TLS-TILT (NL); Elizabeth Coombs, Independent Consultant (AU); Vincent Bouatou, IDEMIA (FR); Oskar Gstrein, Campus Fryslân (NL)

The EU is the first 'global player' to propose a legal framework for the development and use of AI. The EU AI Act adds another layer of regulation for the governance of data infrastructures, which are also addressed by GDPR and other EU instruments. This panel discusses and considers the impact of this overhauled governance framework. The central question is whether the proposed AI governance framework is capable of comprehensively and effectively addressing concerns around privacy and autonomy which arise during the development and use of AI systems. The speakers share observations on gender and stigmatisation, group autonomy and abnormal justice, as well as security (Facial Recognition and Predictive Policing). These sectoral perspectives open a more holistic discussion on how much governance of AI is desirable/needed and whether the EU approach to AI governance will establish a global benchmark.

- How should AI governance address group interests, group privacy and abnormal justice?
- How can governance mechanisms mitigate automated stigmatisation and discrimination related to gender?
- What does the use of live facial recognition mean for 'public' space, and should police be allowed to test these biometric technologies in real settings?
- How will the design and deployment of predictive policing systems be affected by the EU AI Act?

11:45 – ASSESSING THE IMPACT ON FUNDAMENTAL RIGHTS IN AI APPLICATIONS

Academic ☆ **Business** ☆☆ **Policy** ☆☆

Organised by Politecnico Di Torino (IT)

Moderator Anna Buchta, European Data Protection Supervisor (EU)

Speakers David Wright, Trilateral Research (UK); Francesca Fanucci, The Conference of International Non-Governmental Organisations of The Council of Europe (INT); Alessandro Mantelero, Polytechnic University of Turin (IT); Cathrine Bloch Veiberg, Danish Institute for Human Rights (DK)

Digital innovation has reshaped society, benefiting it, but also raising critical issues. These issues have often been addressed by data protection laws, but recent applications of AI have shown a wider range of potentially affected interests. A broader approach focusing on the impact of AI on fundamental rights and freedoms is therefore emerging. Several provisions in the draft EU regulation on AI and in international and corporate documents push in this direction, but do not outline concrete methodologies for impact assessment. Moreover, existing HRIA models are not easily replicable in the AI context. This is despite the important role of such an assessment in relation to the risk thresholds in regulatory proposals. The panel will discuss how fundamental rights can be effectively put at the heart of AI development, providing concrete solutions for a rights-oriented development of AI.

- Are there different types of AI risk assessment and, if so, what are they?
- Who should be entrusted with conducting HRIAs, when and how?
- What are the key criteria that fundamental rights impact assessments need to fulfil to achieve the intended goals?
- How can the HRIA be operationalised in the context of AI by providing measurable thresholds for risk management and human rights due diligence?

13:00 - LUNCH

14:15 – EU CLOUD CODE OF CONDUCT: 1 YEAR ANNIVERSARY - OPERATIONALISING GDPR COMPLIANCE

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Workday

Moderator Frank Ingenrieth, SCOPE Europe (BE)

Speakers Barbara Cosgrove, Workday (US); Carmen Schmidt, Volkswagen (DE); David Stevens, APD-GBA (Belgian Data Protection Authority) (BE); Witte Wijsmuller, DG CNECT (EU)

Nowadays, businesses are faced with an increasingly complex privacy landscape. In particular, those companies involved in international data transfers find themselves in need for more clarity and transparency of rules. Codes of conduct as co-regulatory instruments not only have an ability to react quickly to a fast-past environment that is the current reality but also have a potential to harmonize privacy practices globally. An example of a cloud of conduct that was designed to meet these objectives is the EU Cloud Code of Conduct – the first legally operating code of conduct under art. 40 of the GDPR. During this session the representatives of the regulators, academia, and businesses will discuss in detail how code of conducts support companies in their day-to-day compliance as well as explore the advantages of co-regulatory tools and their potential to address recent challenges with international data transfers.

- What are the advantages of co-regulatory instruments?
- How does the EU Cloud Code of Conduct support the day-to-day compliance of Cloud Service Providers?
- What is the Third Country Transfer Initiative and how can it help address some of the recent challenges with international data transfers?

15:30 - COFFEE BREAK

16:00 – GDPR CERTIFICATION SCHEMES: GENERAL VS. SPECIFIC SCHEMES – WHAT DO EFFECTIVE SCHEMES LOOK LIKE?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Alexander Von Humboldt Institute for Internet and Society (DE)

Moderator Eric Lachaud, Privacy Consultant (FR)

Speakers Max Von Grafenstein, Alexander Von Humboldt Institute for Internet and Society (DE); Jana Krahforst, Usercentrix (DE); Chris Taylor, ICO (UK); Sebastian Meissner, EuroPriSe Certification Authority (DE)

The EDPB has recently published its Addendum to Guidelines 1/2018 on certification and identifying certification criteria per Articles 42 and 43 GDPR and, on this basis, conducted a public consultation process. One key question has been how a scheme must specify the GDPR-provisions with respect to a predefined processing operation. Promoters of general schemes argue that general schemes are more flexible and cost-saving. To the contrary, promoters of specific schemes argue that specific schemes are actually more cost-saving and, above all, are the only way to effectively increase transparency and an EU-wide consistent application of the GDPR. The proposed panel gives an overview of the certification schemes approved so far by Data Protection Authorities or the EDPB and evaluates them against the regulatory objectives of Articles 42 and 43 GDPR.

- What are the regulatory objectives of Articles 42 and 43 GDPR?
- What are the pros and cons of general and specific certification schemes?
- What schemes have been approved by data protection authorities/EDPB so far?
- How far do these certification schemes meet the regulatory objectives?

17:15 – THE AI ACT AND THE CONTEXT OF EMPLOYMENT

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆

Organised by European Trade Union Institute (EU)

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

Speakers Aida Ponce del Castillo, ETUI (BE); Diego Naranjo, EDRI (BE), Paul Nemitz, European Commission (EU), Simon Hania, Uber (NL)

The EC's AI Act proposes a regulatory approach to the use of AI systems. It does not address the specificities of employment and the protection of fundamental and workers' rights. In its current version, it is not designed to deal with the privacy and data protection risks of AI, but to promote the growth of a European AI sector, in line with the EC's oftentimes stated ambition to make the EU a global AI leader. Civil society actors, MEPs and the EDPS have asked the EC to ban remote biometric identification technologies in public spaces. Others, in particular the labour movement, are concerned about the abuse of surveillance technologies in the workplace. How to balance promoting AI and protecting people's rights? This and other essential questions such as -absence of redress mechanisms, liability, governance - will be addressed in this panel discussion.

- Can the AI Act address the specificity of AI uses in employment, including platform work?
- How to balance promoting AI and protecting people's rights?
- Can the AI Act clearly ban both mass surveillance and worker surveillance?
- How can GDPR be effectively implemented in the context of employment?

CPDP2022 PANELS AT AREA 42 MIDI

08:45 – DATA PROTECTION REGULATION POST-COVID: THE CURRENT LANDSCAPE OF DISCUSSIONS IN EUROPE, THE US, INDIA AND BRAZIL

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by Data Privacy Brasil Research Association (BR)

Moderator Bruno Bioni, Data Privacy Brasil Research Association (BR)

Speakers Teki Akuette Falconer, Africa Digital Rights Hub (GH); Gabriela Zanfir-Fortuna, Future of Privacy Forum (US); Malavika Raghavan, Daksha Fellowship/Future of Privacy Forum (IN); Isabelle Vereecken, European Data Protection Board (EDPB) (EU)

Approaches to data protection (or privacy) regulation vary widely, with differences that can be challenging to navigate and pose the question of how to attain minimal regulatory convergence. At the same time, rapid changes, that have been intensified by the emergence of COVID-19, spark other concerns, related to the very ability of data protection legislation to tackle issues such as discriminatory profiling, for example. These are some of the elements of an effervescent scenario that will benefit from a panel with different sectoral and regional perspectives, distributed between Global North and South - namely from the US, the EU, Brazil and India.

The motto of the session is: how have the legal, technological and societal changes precipitated by COVID-19 impacted discussions about data protection regulation around the world?

- Considering contexts, legal systems and regulatory stages in each different country/region represented in the panel, what is the main challenge each one currently faces in safeguarding privacy and data protection?
- Regulatory convergence does not mean replication, but rather synergy. To what extent do particular characteristics of the regulatory environment of each country/region play a role in the choices and possibilities of regulation and enforcement?
- Between government regulation and industry self-regulation there is co-regulation, an approach that is explicitly endorsed by GDPR, as well as the Brazilian General Data Protection Law. Considering the ongoing regulatory discussions in other places such as the US and India, is it possible to say that the latest generations of data protection laws converge to a co-regulation model?
- As technology advances, the notion that traditional data protection regulation is not capable of adequately dealing with some of its challenges is reflected in the introduction of more specific legislation and standards, such as in the field of A.I. What is the current status of this movement in each different country/region and how do all of these different approaches relate in seeking greater protection for individuals and groups?

10:00 - COFFEE BREAK

10:30 – DPAs IN THE COVID-19 PANDEMIC

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by CPDP

Moderator Ivan Szekely, Central European University (HU)

Speakers Charles Raab, University of Edinburgh (UK); Orsolya Reich, Civil Liberties Union for Europe (DE); Hielke Hijmans, Data Protection Authority (BE); Sjaak Nouwt, Royal Dutch Medical Association (NL)

During the COVID-19 pandemic, contact-tracing, data sharing, de-anonymisation and re-identification, and the collection of personal data for testing and tracing (e.g., by bars and restaurants) became the widespread practice of governments, health authorities, and commercial enterprises. DPAs' statutory role as advisers and supervisors regarding these information practices was put to the test. The panel will explore the relations during the pandemic between DPAs and government and scientific/medical advisers, health services, and the conflict between the public interest in data protection and the public interest in health. It will examine whether DPAs could exert their authority as inevitable actors in decision-making concerning the processing of personal data, whether they pressed for the use of Privacy-enhancing or Privacy-by-Design technologies in pandemic control strategies, and whether they have had a say in arbitrating the relationship between information rights and emergency measures.

- Have DPAs been involved in COVID-19 related decision-making?
- Have they been under pressure not to interfere with government and public health solutions?
- If so, how have they responded to this challenge?
- Did data subjects turn to DPAs in COVID-19 related cases?

11:45 – DATA PROTECTION CONCERNS IN THE AML/CFT FRAMEWORK

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆

Organised by Tilburg Institute for Law, Technology, and Society (TILT) (NL) and Digital Legal Studies (DLS)

Moderator Juraj Sajfert, Vrije Universiteit Brussel (BE)

Speakers Eleni Kosta, Tilburg Institute for Law, Technology, and Society(TILT)Tilburg University (NL); Philip de Koster, FIU Belgium (BE); Lora von Ploetz, Commerzbank (DE); Benjamin Vogel Max Planck Institute for the Study of Crime, Security and Law (DE)

The Anti Money Laundering (AML) and Countering the Financing of Terrorism (CFT) framework entails the collection and exchange of information between customers, obliged entities, Financial Intelligence Units (FIUs) and law enforcement authorities, as well as intelligence services in some cases. Such exchanges usually encompass personal data, the protection of which needs to be respected. The need to align the AML/CFT requirements with the data protection ones is essential for the effective and legally compliant functioning of the AML/CFT framework.

- Under which conditions is the exchange of data between the various actors allowed?
- What are the rights of the data subjects when their personal data are processed for AML/CFT purposes?
- What safeguards need to be in place for the facilitation of transfers of data from the EU to third countries in the context of AML/CFT activities?
- What are the major data protection concerns that arise regarding the exchange of data in PPPs in the AML/CFT field?

13:00 - LUNCH

14:15 – SECONDARY USE OF PERSONAL DATA FOR (BIOMEDICAL) RESEARCH

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆

Organised by CiTiP, KU Leuven (BE)

Moderator Griet Verhenneman, CiTiP, KU Leuven (BE)

Speakers Véronique Cimina, EDPS (EU); Tamas Bereczky, Patvocates (DE); Teodora Lalova, CiTiP, KU Leuven (BE); Marina Markatou, One Trust (UK)

Biomedical research relies on the patients' participation and on the use and reuse of special categories of personal data, such as data concerning health. The fight against COVID-19 caused several official bodies to emphasise that the General Data Protection Regulation (GDPR) is not intended to hinder the secondary use of personal data for the purpose of scientific research. However, variation in national interpretation of the GDPR have led to a fragmented approach, which brings uncertainty for researchers and potentially stifles innovation. Questions remain as regards to the interplay of the GDPR with the intricate legal framework applicable to biomedical research. Moreover, several future legislative acts – such as the Data Governance Act and the European Health Data Space – despite their promise to foster the use and reuse of data, could all potentially present novel challenges as regard the protection and use of personal data.

- Individual autonomy versus public interest. Is it database ownership that spurs the discussion in the field of (biomedical) research? Are controversies triggered through the debate on patients' ownership of data?
- When personal data are re-used for scientific research, which safeguards are needed? Do these safeguards depend on the type of controller? Do you consider the same safeguards when the data are sensitive data, e.g. relating to health or genomic data?
- On the interplay of other legal frameworks with the GDPR we ask our speakers to zoom in on one specific framework and discuss the challenges and future considerations. Such frameworks could include the Clinical Trials Regulation, as well as the proposal for a Data Governance Act, and the future European Health Data Space regulation.

15:30 - COFFEE BREAK

16:00 – SHARING THE DIGITAL ME – A CONTEXTUAL INTEGRITY APPROACH FOR DISCUSSING GOVERNANCE OF HEALTH AND GENETIC DATA IN CYBERSPACE

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by Uppsala University (SE) and the CyberGovernance project (University of Oxford (UK), University of Oslo (NO), Uppsala University (SE), University of Iceland (IS), EURAC research)
Moderator Joseph Cannataci, UN Special Rapporteur on the Right to Privacy (MT)
Speakers Deborah Mascalonzi, Uppsala University (SE); Heidi Beate Bentzen, University of Oslo (NO); Mario Jendrossek, The EU Health Dataspace (EU); Christine Beitland, Microsoft Norway (NO)

The European Health Data Space is a step forward for the effective exploitation of Health Data, moving decisively from the concept of ‘open access’ towards ‘open science’. The strong push in the scientific community towards open science already made health and genetic data in research databases available for (re)use by diverse players but not in all the novel contexts where data are going to be used. The governance of Health Data in Cyberspace was scrutinized at different levels from different actors on the theoretical and empirical level. In this panel we will discuss governance directions for the use health-relevant data, looking at results from preference studies conducted with experts and the general public in 12 EEA countries. Results revealed divergences from the GDPR to be discussed with relevant experts. Those results can enrich the discussion for new approaches to governance of data, further conceptualized, in relation to unintended consequences, protection of fundamental rights and societal acceptability.

- What are studies on preferences for the use of health data showing to us?
- What are the elements to be taken into account to reconceptualize open access and open science (taking people preferences into account)?
- What role plays the contextual integrity framework to think governance further?
- Is data driven research taking the human rights framework into account?
- How can we account for responsible science and human rights approaches?

17:15 – MANIPULATIVE DESIGN PRACTICES ONLINE: POLICY SOLUTIONS FOR THE EU AND THE US

Academic ☆ **Business** ☆ **Policy** ☆☆☆
Organised by TACD (EU/US) and Norway Consumer Council (NO)
Moderator Anna Fielder, Transatlantic Consumer Dialogue (EU/US)
Speakers Finn Lützow-Holm Myrstad, Norway Consumer Council (NO); Commissioner Rebecca Slaughter, Federal Trade Commission (US); Kat Zhou, Design Ethically (SE); Kim van Sparrentak, Member of the European Parliament (EU)

Deceptive design practices, or ‘dark patterns’, are used to make consumers take actions against their own interests, to the benefit of companies. Common privacy-invasive dark patterns include hidden default settings that maximise data collection, ambiguous language designed to confuse, and consent flows that push toward certain choices. Such practices are particularly damaging in the context of the surveillance economy, when used by the large platforms to increase their market power. The harms caused by dark patterns are not distributed evenly and have a higher impact on people in vulnerable situations, those with low incomes, children, the elderly, or those with disabilities. Existing policies, such as the GDPR in the EU or US FTC’s section 5 regulations, are not fully equipped to deal with manipulative design practices at scale. However, legislative initiatives are taking place on both sides of the Atlantic.

- What are the drivers/business objectives of ‘dark patterns’?
- How can dark patterns impact individuals and society generally?
- What policy solutions are needed internationally to deal with such practices?
- Will (and how) AI technologies affect dark patterns in the future?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

CPDP2022 PANELS AT AREA 42 PETITE

08:45 – PROTECTING THE RIGHTS AND ENSURING THE FUTURE OF GENERATION AI

Organised by AI4Belgium
Moderator Carl Mörch, FARI - AI For the Common Good Institute (ULB-VUB) (BE)
Speakers Eva Lievens, Faculty of Law & Criminology of Ghent University (BE); Liliana Carrillo, CollectiveUP, SP&CO (BE); Maud Stiernet, World Wide Web Consortium (W3C) (BE); Leyla Keyser, Bilgi university (TR); Klara Pigmans, Delft University of Technology, Consultant for UNICEF (NL)

Any child born today will be impacted by Artificial Intelligence. It is everywhere, from children’s video games to their classrooms, from their smartphones to their online social platforms. This can be positive, as teaching children about this technology could enable them to do incredible things with it. But there are also potential adverse effects. Intentionally or not, this technology can be used to their detriment, and put at risk their rights and interests - such as their privacy, autonomy and well-being. In this session, we would like to dive into the details of how to help ensure that children can enjoy the benefits of artificial intelligence, while ensuring that their human rights are protected. The panel will therefore focus on the specific risks associated with AI and children, but also on how we can properly empower them as members of the so-called “AI generation.”

- What are the major concerns when using AI in relation to children?
- Any child born now will be influenced by AI; how do we ensure that the deployment of AI takes into account the children’s fundamental rights?
- How could we guarantee that the rights and interests of children are prioritised (e.g. over commercial or other interests) when designing AI systems?
- What role does education play in protecting the rights of children? How can we improve AI literacy? What are the roles of parents and educators in this regard?

10:00 - COFFEE BREAK

10:30 – REGULATING AI IN HEALTH RESEARCH AND INNOVATION

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆☆
Organised by Department of Innovation and Digitalisation in Law, University of Vienna (AT)
Moderator Tima Otu Anwana, University of Vienna (AT)
Speakers Max Königseder, MLL Meyerlustenberger Lachenal Froriep AG (CH); Richard Rak, University of Bologna (IT); Mariana Risetto, University of Vienna (AT); Elisabeth Steindl, University of Vienna (AT); Martin Urban, Boehringer Ingelheim (DE)

AI systems in healthcare can help diagnose disease, prevent outbreaks, discover treatments, tailor interventions and enable Internet of Health Things devices. However, the use of AI raises questions about the proper interpretation, application and interplay of EU regulations in force (GDPR, MDR/IVDR) and new legislative initiatives (AIA, European Health Data Space). The panel will debate critical data protection and AI governance challenges regarding the development and use of AI systems in health innovation and research. The speakers will discuss regulatory and governance affairs for AI-supported medical and consumer health devices, with a particular focus on mental health applications. In addition, the discussion will address consent mechanisms, anonymisation and related risk mitigation measures concerning the use of AI in healthcare and explore the possible implications of regulating AI in light of the foreseen European Health Data Space.

- What are the possible implications of the AIA for the innovation of Internet of Health Things devices and interconnected AI systems?
- Is implementing privacy by design and fostering privacy-enhancing technologies the better way to enable health research on the basis of consent?
- What are the concerns of using data-driven technologies in medical & consumer health devices intended to be used for mental health purposes?
- What are the legal challenges and risks concerning the anonymisation of health data and how to mitigate the risks associated with re-identification?

- Is the interplay between the AIA and the European Health Data Space initiative enough to establish a clear set of rules applicable to AI in health research?

11:45 – A SANDSTORM OR JUST A BREEZE? WHAT’S THE FUSS ABOUT SANDBOXES?

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆

Organised by The Norwegian Data Protection Authority (Datatilsynet) (NO)

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

Speakers Kari Laumann, Norwegian Data Protection Authority (NO); Chris Taylor, ICO, (UK); Erlend Andreas Gjære, Secure Practice (NO); Dragos Tudorache, MEP (EU)

Artificial intelligence (AI) offers enormous potential for better, personalised and more efficient services. At the same time AI is data intensive and often challenges basic privacy principles. Can you have your cake and eat it too? This panel will explore the opportunities and limitations of sandboxes as a tool for fostering innovative and responsible AI solutions. The panelists include both regulators and sandbox participants who will share their experiences from the first data protection sandboxes in Europe. The panel will also discuss the role of sandboxes in the proposed AI Act.

- Are sandboxes the right tool to foster responsible innovation?
- Do sandboxes effectively help AI companies overcome regulatory barriers?
- What are the main learnings from the first round of data protection sandboxes in Europe?
- Will everyone have a sandbox in a few years? Are sandboxes the future when it comes to regulating algorithms?

13:00 - LUNCH

14:15 – THE RETURN OF PRIVACY? ‘SMART VIDEO SURVEILLANCE’ EVALUATING DATA PROTECTION IN THE LIGHT OF PRIVACY AND SURVEILLANCE

Academic ☆☆☆☆ **Policy** ☆☆

Organised by VUB Chair in Surveillance Studies (BE)

Moderator Rosamunde van Brakel, University of Tilburg/VUB (NL/BE)

Speakers Ola Svenonius, Swedish Defense College (SE); Bryce Newell, University of Oregon (US); Lilian Edwards, Newcastle Law School (UK); Fanny Coudert, EDPS (EU)

In 1995, a US philosopher Jeffrey Reiman warned for the risks to privacy posed by the then novel Intelligent Vehicle Highway System. In the same year in the UK, criminologist Clive Norris raised concerns about algorithmic surveillance in the form of emerging facial recognition and ANPR cameras. Almost thirty years later, that future is now a reality and the world is connected in unprecedented ways facilitated by the ubiquitous proliferation of ‘smart’ surveillance cameras. Efforts to address these concerns side-tracked the discussion to issues of data protection, an outcome at least in theory more easily measurable and enforceable. However, when looking at ‘smart’ video surveillance practices in Europe, it becomes clear that regardless of data protection regulation, these have proliferated also beyond security and crime prevention purposes (often in the context of smart cities) and are becoming normalized. It seems that ‘old-fashioned’ privacy and surveillance concerns have been replaced by narrow data protection compliance. Moreover, societal concerns of surveillance, such as social sorting and changing power relations have become even more pertinent with advancements of Big Data and AI, demanding a broader framework that can incorporate collective and societal harms.

In this regard, The VUB Chair in Surveillance Studies panel aims to discuss privacy and data protection in the context of smart video surveillance by asking the following questions:

- What are the main individual, collective and societal harms of smart video surveillance?
- Does data protection regulation undermine privacy and act as an enabler of smart video surveillance?
- Does the proposed AI regulation address ‘old-fashioned’ privacy and surveillance concerns of smart video surveillance?
- How can privacy and surveillance concerns regain importance in data protection policy?

15:30 - COFFEE BREAK

16:00 – ENCODING IDENTITIES: THE CASE OF COMMERCIAL DNA DATABASES

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆

Organised by University of Amsterdam (NL)

Moderator Alexandra Giannopoulou, Institute for Information Law (IViR) (NL)

Speakers Amade M’Charek, University of Amsterdam (NL); Rossana Ducato, University of Aberdeen (UK); Taner Kuru, University of Tilburg (NL); Ella Jakubowska, EDRI (BE)

This panel aims to enable an interdisciplinary discussion on the legal and normative aspects of digital identities operating on a global scale. We focus on the use of commercial genealogical DNA databanks stemming from –oft US-based- private companies for criminal investigations all over the world. Namely, we attend to the convergence between surveillance, forensics and direct to consumer DNA technologies. This case is particularly salient because it ties together the rapid rise, and intensive use of biometric identifiers, the commodification of digital identities, and the use of recreational identity services in criminal investigations. The objective in unravelling this practice of converging technologies and uses, is to problematize digital identities, to examine how they become something else when mobilized for different purposes on a planetary scale, and what the social and legal consequences thereof are.

- What are the legal, social, and institutional environments enabling the production of identities produced through commercial DNA services?
- How are the technologies enabling the creation of these dafied genomic profiles altering existing perceptions of citizenship and -ultimately- of identity?
- What are the implications of the convergence of different, formerly geographically, legally, normatively isolated systems, uses, and practices around (digital) identities?

17:15 – EFFECTIVE TRANSPARENCY AND CONTROL MEASURES (INCLUDING PRIVACY ICONS): THE EXAMPLE OF COOKIE BANNERS. WHERE DO WE STAND NOW?

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Einstein Center Digital Future / Berlin University of the Arts (DE)

Moderator Max von Grafenstein, Einstein Center Digital Future/Berlin University of the Arts (DE)

Speakers Estelle Hary, CNIL (FR); AbdelKarim Mardini, Google (FR); Jana Krahforst, Usercentrix (DE); Nina Herbort, Berlin Data Protection Authority, European Data Protection Board (EDPB) Cookie Banner Task Force (DE)

Cookie consents with manipulative information and decision architectures are ubiquitous, at least perceived to be. The problem of such so-called dark patterns has long been recognised by regulators, studied by scientists and now also fought by data protection activists. But what are positive examples of particularly successful transparency and control measures? On what methodological basis can these be developed, and their effectiveness tested? And what is the current state of research and development of privacy icons that are considered part of the solution? The panel will provide an overview of examples from (law enforcement) practice and the current state of research as well as possible development paths.

- What are the most recent/prominent examples of good and bad transparency and control measures in practice?
- Which approaches exist in research to design and test good transparency and control measures?
- Which role do PIMS, CMP and browsers play in this context?
- What is the regulator’s point of view on this?

18:30 – COCKTAIL SPONSORED BY EDPS

in Le Village

07:30 - Registration in La Cave
08.15 - Welcome coffee in Le Village

CPDP2022 PANELS AT GRANDE HALLE

08:45 – CONVERGENCE IN ACTION: REGIONAL AND GLOBAL COOPERATION BETWEEN DATA PROTECTION AUTHORITIES

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by European Commission (EU)
Moderator Aissatou Sylla, Hogan Lovells (FR)
Speakers Waldemar Gonçalves Ortunho Junior, Data Protection National Authority (BR); Tamar Kaldani, CoE Consultative Committee of the Convention 108 & Former Data Protection Commissioner of Georgia (GE); Joaquín Pérez Catalán, Spanish Data Protection Agency (ES); Drudeisha Madhub, Data Protection Office of Mauritius (MU)

Data Protection Authorities - established and nascent - are increasingly engaging in cross-border cooperation. Regional and global networks are seen not only as providing opportunities to share knowledge, exchange best practices or enhance enforcement cooperation, but also as a means to foster convergence around high data protection standards. At the same time, new synergies are developing between these networks and international organisations such as the OECD, ASEAN, or the EU, whose work focusses increasingly on developing bridges between different privacy systems, to facilitate trusted data flows.

On this panel, regulators, and privacy specialists from across the globe will share their views on the benefits, challenges, and potential of cross-border cooperation between data protection authorities, including what citizens and business stand to gain from it. We will learn about the practical experience of authorities that have engaged in this type of cooperation and hear the expectations of recently established ones. We will also discuss new forms of cooperation at regional and global level.

- What are the benefits of cross-border cooperation between DPAs and what are the challenges to the (further) development of such cooperation?
- What can regional networks do to bring cooperation between DPAs to the next level? What are the success stories and missed opportunities for regional cooperation?
- How can national, regional and global frameworks interact better in order to foster convergence in privacy standards? Is cooperation between regional networks a realistic objective, in addition or as an alternative to bilateral cooperation?

10:00 - COFFEE BREAK

10:30 – GLOBAL GOVERNANCE OF PRIVACY: BEYOND REGULATION

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Apple (US)
Moderator Jane Horvath, Apple (US)
Speakers Erik Neuenschwander, Apple (US); Alexander Hanff, Privacy Advocate (SE); Konstantin Böttinger, Fraunhofer AISEC (DE); Anna Buchta, European Data Protection Supervisor (EU); Lorenzo Dalla Corte, Tilburg University (NL)

Privacy has increasingly become front page news, featuring prominently in political and social debates and financial reporting. From the legislative side, this is driven by laws such as the GDPR (EU), CCPA (CA), LGPD (BR) and PIPL (CN). But privacy is also being shaped by industry itself and beyond local legal requirements, with industry-led privacy enhancing technologies enabling global privacy effects. Civil society has also played a pivotal role in privacy governance, where academics and activists exert influence on privacy regulation and business practices. More and more, multistakeholderism is shaping global perspectives of privacy and reframing roles in this space. The panel will seek to explore how privacy and privacy enhancing technologies are being realized through multistakeholderism and the pros and cons of this approach. Can technical solutions to privacy pave the way for high levels of privacy protection beyond jurisdictional borders? Should laws provide space or even incentives for privacy preserving innovation and, if so, how? Panellists will be asked to put forward their views on global

governance of privacy and whether privacy can and should be achieved through multistakeholderism and the limits therein.

- Can laws on their own achieve enhanced privacy for individuals?
- What are the areas for collaboration that can identify and achieve privacy paradigm shifts?
- How do we do so in a manner that enhances privacy without causing stakeholders to seek to block or water down those changes?
- What role will technology developments play and how can we harness those developments for good?

11:45 – LEVERAGING AI: RISKS & INNOVATION IN CONTENT MODERATION BY SOCIAL MEDIA PLATFORMS

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Meta
Moderator Aleksandra Kuczerawy, KU Leuven (BE)
Speakers Nicola Aitken, Meta (IE); Eliska Pirkova, Access Now (BE); Guido Lobrano, ITI (BE); Eva Maydell, MEP (EU)

Businesses and organisations rely on AI to innovate, and increasingly rely on AI to protect the public interest. For social media platforms, AI can be a powerful tool for content moderation in order to keep users and the public safe, for instance by detecting and taking down violating content and accounts. At the same time, social media platforms need to preserve privacy, fairness, and freedom of expression. Content moderation does not come with a one-size fits all approach. Panelists will dive into how AI-based detection of illegal and harmful content works in different areas of harm, such as hate speech, child safety or illegal content. The panel will also discuss the risks and safeguards, transparency, control, privacy, fairness, and the role of human review and intervention. Some of the questions that will be addressed are:

- Which data is needed for AI to be effective in different areas of harm, such as hate speech, misinformation, or illegal content?
- What are the opportunities and risks of leveraging AI, and which challenges need to be addressed for AI to be effective and safe for content moderation?
- Which other industry use cases could leverage AI for content moderation?
- How can regulation optimise for effective and safe use of AI for content moderation?

13:00 - LUNCH

14:15 – RE-FRAMING DATA USE: VALUES, NORMS, INSTITUTIONS

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by The Ditchley Foundation (UK)
Moderator James Arroyo, The Ditchley Foundation (UK)
Speakers Julie Brill, Microsoft (US); Jan Philipp Albrecht, Minister for Energy, Agriculture, the Environment, Nature and Digitalisation of Schleswig-Holstein (DE); Bruno Gencarelli, European Commission (EU); Sir Julian King, Flint Global (UK)

This will be a panel discussion that reframes the central role of data to society and examines duty of care in an era where we need to enable responsible data use globally. For societies to flourish in the 21st century, government, civil society, and industry will need to invest in the appropriate use, maintenance and regulation of data while remaining committed to maximizing the societal benefit and protecting fundamental rights. The panel will examine current and future norms around the use of data globally and how policy, technical innovation and operational controls can protect the trusted free flow of data in health care, trade and government access while protecting privacy and human rights.

- What are current norms concerning the use of data globally?
- What are possible future norms concerning the use of data globally?
- How can policy appropriately protect the trusted free flow of data?
- How can technical and operational controls appropriately protect the trusted free flow of data?

15:30 - COFFEE BREAK & CNIL-INRIA PRIVACY AWARD, EPIC CHAMPION OF FREEDOM AWARD

16:00 – INNOVATION IN CYBERSECURITY - ACCELERATING EUROPE'S DIGITAL TRANSFORMATION AND DIGITAL RESILIENCE THROUGH STRONGER PARTNERSHIPS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Google

Moderator Chris Kubecka, HypaSec and Middle-East Institute (US/NL)

Speakers Tatyana Bolton, R Street Institute (US); Heli Tiirmaa-Klaar, Digital Society Institute, ESMT Berlin (DE); Philipp Amann, European Cybercrime Centre, Europol (EU); Wieland Holfelder, Google Cloud Security (DE)

How can we further strengthen collaboration in the field of cybersecurity to establish more effective public-private partnerships and collectively increase our digital resilience? The scale of the challenges that we face in cyberspace today is enormous, constantly evolving and too large for any one organization or country to tackle alone. Cybersecurity is a file that is strengthened by scale and through international collaboration. Developing a global model that forges partnerships around a common view of cyber-risk, coordinated incident detection and response, information sharing, innovation, capacity building and alignment on global rules and standards has never been more important. The panel will address how partnerships between industry, the public sector, civic society, academia and technical experts can be deepened to meet our shared cybersecurity challenges more effectively, moving also from a reactive to a proactive response. Examples will include the networked approach established by Europol.

- How can privacy by innovation and privacy-enhancing technologies like homomorphic encryption contribute to more cyber resilience and strengthen public-private collaboration?
- Is the focus on cybersecurity enough or do we need a more comprehensive digital resilience-approach?
- Information sharing is the current demand but what are the limits and challenges caught between privacy and law enforcement needs?
- How can we respond to threats in cyberspace more proactively?

17:15 – DATA PROTECTION AND HIGH-TECH LAW ENFORCEMENT – THE ROLE OF THE LAW ENFORCEMENT DIRECTIVE

Academic ☆☆ **Business** ☆ **Policy** ☆☆☆

Organised by EU Agency for Fundamental Rights (FRA) (EU)

Moderator Elise Lassus, FRA (EU)

Speakers Zoi Kardasiadou, DG JUST (EU); Griff Ferris, Fair Trials (UK); Juraj Sajfert, VUB (BE); Julia Ballaschk, Danish National Police, Center for Data Protection (CfD) (DK)

In 2022, the European Commission will deliver its first evaluation and review of the Law Enforcement Directive (LED). While adopted simultaneously to the General Data Protection Regulation (GDPR), this Directive did not – at the time – receive the same level of attention as the GDPR did. However, technology for law enforcement and surveillance purposes is increasingly being used, or considered for use, with limited awareness of the full scope of its potential impact on individuals' rights and freedoms. Moreover, the technologies available to law enforcement authorities are continuously diversifying, from predictive policing to the use of drones, facial recognition technologies, or smart cameras. This creates new challenges for law enforcement officers and rights defenders alike.

Focusing on the Law Enforcement Directive, this panel will provide an opportunity to reflect on the data protection legal framework applying to the use of technologies for law enforcement purposes, and its application to current challenges. Building on their professional experience and expertise, invited panellists - academics, policymakers and law enforcement officers - will discuss how the existing data protection legal framework applies to law enforcement with respect to the use of new technology, and whether this framework adequately ensures fundamental rights.

- What sort of new technologies are used for policing and what are the main issues and concerns raised?
- What are the specificities and challenges of applying data protection principles in the law enforcement context?
- To which extent can the principle of transparency be safeguarded, to make sure that individuals are aware of the use of technologies for law enforcement purposes, and have access to effective remedies when necessary?
- How are the legitimacy, necessity and proportionality of law enforcement technological tools assessed?
- Are current oversight mechanisms sufficient to protect individual's fundamental rights – and notably the right of access to effective remedies?

18:30 – COCKTAIL SPONSORED BY EPIC in Le Village

CPDP2022 PANELS AT LA CAVE

CPDP Global is a new, full-day addition to the CPDP programme on Tuesday 24 May. It is designed to spotlight the latest developments and conversations on data protection, privacy, and technology from around the world. CPDP Global will be livestreamed and accessible online, so that those who cannot physically attend the conference can still connect with the CPDP community. The online track will also be screened for the CPDP in-person audience at La Cave. Both the on and off line audience will be able to interact.

07:30 – DATA PROTECTION FRIENDSHIP: THE EU AND JAPAN [CPDP GLOBAL]

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Chuo University (JP)

Moderator Hiroshi Miyashita, Chuo University (JP)

Speakers Kazue Sako, Waseda University (JP); Naoko Murai, Journalist (JP); Hinako Sugiyama, Independent Consultant (US); Laura Drechsler, Vrije Universiteit Brussel (BE)

This panel will examine the recent data protection law reforms in Japan and consider the convergence between Japan and the EU. The 2019 adequacy decision for Japan was a success story for constructing privacy bridges between the EU and Japan. Furthermore, the Act on the Protection of Personal Information (APPI) was amended in 2020 and 2021, with major changes in its legal regime, with a GDPR influence. While the EU and Japan mutually declared their friendship regarding data protection in 2019, there are still unsettled and emerging issues. For instance, the EU adequacy decision covers the private commercial sector, in other words, there is no adequacy decision over the public sector for Japan. Japan also has been engaging with other partners such as the U.S. and the U.K. with new trade agreements, which may potentially impact algorithmic transparency and data subjects' rights. With regards to the AI regulation, Japan has not yet prepared its legally binding instruments – unlike the proposed AI regulation. Japan promotes Data Free Flow with Trust, whose trusted framework of data flow is under construction. If a convergence is a matter of degree, it is important to measure its closeness from a scientific perspective. The experts from Japan and Europe will give you their observations on EU-Japan data protection convergence.

- How successfully has the EU exported data protection values to the Far East?
- Does the trade agreement (e.g. Japan-US/ Japan-UK) dilute the solid EU-Japan mutual adequacy decision?
- What is the Japanese ambition of Data Free Flow with Trust (DFFT) initiative?
- How can we realise 'trusted' data flows and what is the Japanese approach of trusted web with verified data exchange?

08:45 – DATAFICATION AND PLATFORMISATION IN ASIA: DATA-RICH AND POLICY-POOR OR VICE VERSA? [CPDP GLOBAL]

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Digital Asia Hub

Moderator Malavika Jayaram, Digital Asia Hub (HK)

Speakers Helani Galpaya, LIRNEasia (LK); Wanshu Cong, The University of Hong Kong Faculty of Law (HK); Nighat Dad, Digital Rights Foundation (PK); Rosa Kuo, Open Culture Foundation (TW)

Asia is a poster child for multiple imaginaries: a laboratory for beta testing surveillance practices; a sandbox for new governance approaches; a shiny futuristic universe of gadgets and super-apps; a backward region with extreme data poverty and digital illiteracy. Yet most narratives treat Asia as a monolith. This all-women panel goes deeper, unpacking the specific ways in which datafication and platformisation across Asia are both enabling and challenging, and their implications for rights, entitlements, and consumer welfare. Highlighting recent legal and policy developments (in China, Pakistan, Singapore, Sri Lanka and Taiwan), this session explores overarching themes of data and policy richness and poverty through multiple lenses – law, public policy, futures thinking, ICT research, and advocacy.

- What are the domestic and international drivers for new legislative approaches? How are consumer interests articulated and incentivised?
- How do women, youth and marginalised groups experience digital platforms differently?
- How do perceptions of surveillance and privacy help or hinder digital and civic participation?
- How does the state see its citizens and improve governance outcomes through data? Are privacy-preserving welfare programs unrealistic in emerging economies?

10:30 – SMART BORDERS? ARTIFICIAL INTELLIGENCE AT THE EU BORDER**Academic** ☆☆☆ **Policy** ☆☆☆**Organised by** Karlsruhe Institute of Technology (DE)**Moderator** Franziska Boehm, Karlsruhe Institute of Technology/ FIZ Karlsruhe – Leibniz Institute for Information Infrastructures (DE)**Speakers** Niovi Vavoula, Queen Mary University of London (UK); Aleksandrs Cepilovs, eu-LISA – European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (EU); David Reichel, FRA – European Agency for Fundamental Rights (EU); Paulina Jo Pesch, Karlsruhe Institute of Technology, research project INDIGO (DE)

Decision-making at the EU borders is supported by technological means. Especially Artificial Intelligence (AI) applications are increasingly explored and used at the EU border. Based on the processing of vast amounts of data such applications shall support border control and the identification of security risks. This raises concerns about fundamental rights and data protection. The panel sheds light on new technological trends in decision-making at the EU border such as models trained with Machine Learning (ML) for biometric identification and the assessments of security, migration or other risks. The panelists address practical problems and fundamental rights issues of the development and use of such technologies and discuss approaches to address the identified concerns and shortcomings of existing law and current practice.

- How can AI applications affect decision-making at EU borders?
- What are the benefits and risks of AI at the EU border? What are the main concerns for fundamental rights?
- Can we align fundamental rights and data protection?
- Do we need further regulation of AI in particular with regard to border policy? If yes, which instruments would be suitable and how should regulation look like?

11:45 – PRIVACY PRESERVING ADVERTISING: PROSPECTS AND PARADIGMS**Academic** ☆ **Business** ☆☆☆ **Policy** ☆☆☆**Organised by** Mozilla**Moderator** Alexander Fanta, netzpolitik.org (AT, BE)**Speakers** Karolina Iwańska, Panoptykon Foundation (PL); Catherine Armitage, AWO (BE); Udbhav Tiwari, Mozilla (AU); Christian D'Cunha, European Data Protection Supervisor (EU)

The current state of the web is not sustainable, particularly in the context of how online advertising works. It is a hostile place for user privacy, and is effectively an arms race between browser anti-tracking technologies and trackers. It's opaque by design, rife with fraud, and does not serve the vast majority of those which depend on it - from publishers, to advertisers, and of course, the people who use the open web. At the same time, there's nothing inherently wrong with digital advertising. It supports a large section of services provided on the web and we believe it is here to stay. However, the ways in which advertising is conducted today - through pervasive tracking, serial privacy violations, market consolidation and lack of transparency - is not working and causes more harm than good. This panel discussion will combine insights from the technical, policy and digital rights landscape, with the goal of educating the audience at CPDP on the role that technical and operational solutions will play in the future of behavioural advertising. In doing so, it will provide guidance for policymakers and policy stakeholders on the realities that need to be accounted for in future regulatory frameworks that seek to restrict certain practices and create opportunities for a more sustainable growth of the Internet's business model.

- What are some of the current industry practices that make behavioural advertising unsustainable from a privacy perspective?
- What are the efforts underway in the web ecosystem to let the current practices take place in a more privacy preserving manner?
- How do these industry efforts relate to the policy developments in the space, including recent moves calling for the ban of behavioural advertising?
- What can advertisers do to improve the health of the online advertising ecosystem?
- What is a way forward that allows the various stakeholders to achieve consensus on some of these issues and allow the web ecosystem to evolve for the better?

14:15 – PERSONAL DATA PROTECTION IN AFRICA AND IN THE MIDDLE EAST: DEVELOPMENTS AND CHALLENGES POSED BY THE PANDEMIC [CPDP GLOBAL]**Academic** ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆**Organised by** CPDP**Moderator** Lahoussine Aniss, Office of the Privacy Commissioner (CA)**Speakers** Marguerite Ouedraogo Bonane, Chairwoman of the DPA of Burkina Faso (BF); Sami Mohamed, Commissioner of Data Protection at Abu Dhabi Global Market (UAE); Mila Romanoff, United Nations Global Pulse (INT); Teki Akuetteh Falconer, Africa Digital Rights Hub (GH); Immaculate Kassait, Commissioner of the Kenyan Data Protection Authority (KE)

Several structuring data-driven projects, requiring massive collection and use of personal data have been initiated in Africa and in the Middle East. These projects are initiated either by national governments, as is the case in the UAE and Qatar, or by continental and international actors such as Smart Africa, the World Bank and the United Nations. A key success factor to the above-mentioned projects is the enactment and efficient enforcement of data protection frameworks that enable digital trust among controllers and data subjects. This panel aims, on the one hand, to shed the light on the development of privacy frameworks in Africa and in the Middle East and, on the other, to examine how DPAs (both established and nascent ones) and other stakeholders (NGOs and UN organizations) adopt these in order to strike the right balance between pressing demands for personal data and individuals' privacy protection, especially when other rights (health, security, etc.) are also at stake.

- What is the current/foreseeable map of personal data protection frameworks in Africa and in the Middle East?
- What are the enablers and hurdles to the development of privacy protection in the region?
- Privacy protection is relatively a nascent concept in the region?
- How do DPAs manage to keep the pace with international development in this field, which are most of time driven by imported technologies?

16:00 – CORPORATE COMPLIANCE WITH A CROSS CONTINENTAL FRAMEWORK: THE STATE OF GLOBAL PRIVACY IN 2022 [CPDP GLOBAL]**Business** ☆☆☆ **Policy** ☆☆☆**Organised by** CPDP**Moderator** Omer Tene, Goodwin (US)**Speakers** Merci King'ori, Future of Privacy Forum (KE); Renato Leite Monteiro, Twitter (BR); Barbara Li, Rui Bai Law (CN); Anna Zeiter, eBay (CH)

In 2022, it is no longer enough to know the latest privacy developments out of Europe or even the United States. Global businesses need to comply with an increasingly expanding scope of privacy and data protection laws, including the PIPL in China and LGPD in Brazil. India is contemplating its comprehensive data protection legislation, while African nations continue to adopt new laws. Even as new countries are joining the fray, numerous nations - including for example Australia, Canada, Israel and Singapore - are in the midst of reforming their data protection frameworks. In this session, experts from five continents discuss the challenges of complying with multiple laws, the additional friction caused by localization requirements and transfer restrictions, and strategies for staying ahead of the curve.

- How are businesses addressing a growing list of data protection law?
- Do localisation requirements and data transfer restrictions threaten the Internet and global trade?
- Emerging enforcement trends of new laws including in China and Brazil?
- How can we compare new frameworks to GDPR and CCPA?

17:15 – OPENING THE DATA OF MONEY: CHALLENGES AND OPPORTUNITIES FOR THE GLOBAL SOUTH [CPDP GLOBAL]

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by Open Knowledge Foundation

Moderator Guy Weress, Civil Society (HU)

Speakers Andrés Arauz, UNAM, México and Dollarisation Observatory (EC); Renata Avila, Open Knowledge Foundation (GT); Burcu Kilic, Minderoo Foundation (TR); Iness Ben Guirat, independent privacy activist (TN)

In the twenty-first century, most money is just data - accounting data. Therefore, the data of money and the information of money should not remain hidden from public scrutiny. The panel will discuss how to make the data of money open while preserving privacy and its relevance to open a new era of active citizens, understanding complex financial systems, and reclaiming global financial data as a commons. This is the point where the transparency and data community and geopolitics meet.

- In the twenty-first century, most money is just data - accounting data -. Therefore, the data of money and the information of money should not remain hidden from public scrutiny. Can we make the data of money “open”?
- The cross-border flow of data of money should become an open standard rather than the exclusive property of monopolistic providers. Is that possible today?
- Cross-border data should follow such a standard and, along with the data of money of national payment systems, should become public assets open to research communities and innovators. Is that possible?
- Which are the challenges to make the data of money more open?

18:30 – REGULATING AI AND PERSONAL DATA IN LATIN AMERICA [TILL 19:45 CET] [CPDP GLOBAL]

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by CPDP

Moderator Danilo Doneda, National Council for Privacy and Data Protection (BR)

Speakers Ana Brian, UN Special Rapporteur for Privacy (UY); Luca Belli, Center for Technology and Society at FGV Law School (BR); Olga Cavalli, SSIG (AR); Veridiana Alimonti, Electronic Frontier Foundation (BR)

In Latin America, after a boost on data protection regulation in the last decade, Artificial Intelligence studies and even regulatory initiatives are increasingly being proposed. Some countries have published or are considering their own AI strategies and the Brazilian Congress is considering a Bill for an AI regulatory Framework, which has already been voted by the Chamber of Deputies. This panel will explore the main regional initiatives on AI, their overlap with data protection, their intersection with human rights law, and the specific regulatory and technological approaches that are emerging and being proposed in the region.

- Latin American countries are studying how to regulate AI. What are the latest developments at the regional and national level?
- AI systems have been deployed at scale in Latin American countries by public and private players alike. Smart Cities initiatives, credit scoring, face recognitions are some of the most common examples. What is the role of data protection in how this initiative are framed?
- What are the key trends in Latin America regarding AI and personal data governance?

20:00 – INNOVATING DATA GOVERNANCE IN LATIN AMERICA [TILL 21:15 CET] [CPDP GLOBAL]

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by CPDP LatAm

Moderator Nicolo Zingales, FGV Law School (BR)

Speakers Fernanda Campagnucci, Open Knowledge Brazil (BR); Natalia Carfi, Open Government Partnership (AR); Renato Leite, Data Privacy Brazil/Twitter (BR); Carolina Rossini, Datasphere (US); Edison Tabra, Pontifical Catholic University of Peru (PE); María Lorena Florez, Universidad de los Andes (CO)

The importance of evidence-based policies is globally acknowledged and such evidence increasingly relies on the use of large (personal) data pools for policy planning. Public and private sector actors alike increasingly depend on personal data

processing to provide their services. For Latin America, the innovative use of personal data for policy planning plays a fundamental role to reduce inequalities. However, some core challenges persist, including how to implement innovative, secure, and legally interoperable data governance systems. This CPDP LatAm panel will explore some flagship initiatives and policies on data governance in Latin America.

- What data-driven responses have we seen to fight the pandemic in Latin America, and have they been effective?
- Are organisations in the region adopting appropriate risk-aware techniques for the disclosure of potentially identifying information?
- Can we identify common patterns amongst initiatives that facilitate effective use of data for policy-planning?

CPDP2022 PANELS AT AREA 42 GRAND

08:45 – SEE YOU IN COURT! – DISCUSSING THE POTENTIAL AND CHALLENGES OF JUDICIAL ACTIONS FOR GDPR INFRINGEMENTS

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆

Organised by Law, Science, Technology and Society (LSTS) Research Group, Articulating Law, Technology, Ethics & Politics Project (ALTEP DP) (BE)

Moderator Johnny Ryan, Irish Council for Civil Liberties/ Open Markets Institute (IE)

Speakers Alexia Pato, University of Girona (ES); Anton Ekker, Ekker Advocatuur (NL); Estelle Massé, AccessNow (BE); Michalina Nadolna Peeters, LSTS (VUB) (BE); Romain Robert, NOYB (AT)

The GDPR has been in force for nearly four years, but the challenges of enforcing it set it up to be a paper tiger. The one-stop-shop seems to benefit companies, underdelivering on the GDPR’s promise to give individuals back control of their personal data. NGOs and individuals start to turn to courts to enforce GDPR-conferred rights, including to compensation. Yet, the divergences between national laws of EU countries make private cross-border actions challenging. National laws may significantly differ as to the burden of proof, the notions of infringement and damage, causality as well as compensation. With no clear rules determining the applicable law there is a growing risk of fragmentation of individuals’ level of protection. The upcoming Collective Redress Directive holds a promise to offset some of the existing challenges and facilitate collective actions, yet comes with its own uncertainties.

- Why going to court might be more effective than going to a DPA?
- Can courts rectify the deficiencies of enforcement via DPAs?
- How do national divergences in substantive and procedural laws impact cross-border private actions?
- What are the specific challenges faced by NGOs when bringing cross-border private actions, and what are the recent private actions launched?
- What is the interlink between the Collective Redress Directive and the GDPR, and does it signal the advent of a new era for GDPR enforcement?

10:00 – COFFEE BREAK

10:30 – CONCRETE AND WORKABLE SOLUTIONS TO THE GDPR ENFORCEMENT

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by NOYB

Moderator Jennifer Baker, EU technology journalist (BE)

Speakers Nina Herbolt, Berlin Supervisory Authority (DE); Gwendal Le Grand, EDPB (EU); Max Schrems, NOYB (EU); Lisette Mustert, University of Luxembourg (LU)

Europe is proud to have the most progressive privacy legislation in the world, however the lack of enforcement leads to legitimate frustration of users and small business. In order to unlock the full potential of the General Data Protection Regulation (GDPR) some of the persisting issues related to its enforcement by Europe’s Supervisory Authorities have to be fixed. The panel is aimed at understanding the underlying issues, as well as identifying concrete and workable solutions with key actors

representing a national supervisory authority, academia, and the European Data Protection Board (EDPB).

- What are the persisting issues in the area of the GDPR enforcement?
- Why do they occur?
- What solutions are there?
- What are the respective roles of the EU Supervisory Authorities, EU institutions, and civil society organisations?

11:45 – INTERDISCIPLINARY DATA PROTECTION ENFORCEMENT IN THE DIGITAL ECONOMY

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆☆

Organised by The European Consumer Organisation (BEUC) (BE)

Moderator Ursula Pachi, BEUC (BE)

Speakers Cecilia Tisell, Swedish Consumer Protection Authority (SE); Isabelle Buscke, vzbv (DE); Hans Micklitz, European University Institute (EU); Tobias Judin, Norwegian Data Protection Authority (NO)

‘Move fast and break things’ has been the motto of some of the biggest tech companies. It can be largely debated what they have actually ‘broken’ but one thing is clear: the lines that separated various areas of law (e.g. competition, consumer protection, data protection) have been broken, or at least blurred. This creates many challenges. How can we effectively address practices which may infringe several legal instruments at the same time, in several jurisdictions, under the watch of several authorities? Bad actors seek to exploit the cracks and gaps in our system and often get away with little consequences for their actions. Whereas the gravity of those actions might sometimes seem limited when looking through a single lens, the picture quickly changes when we broaden our perspective. It is time for enforcers to move fast and break things too.

- How are existing EU enforcement structures in various areas cooperating with each other?
- How can we achieve effective interdisciplinary enforcement to tackle systemic issues undermining our rights and freedoms in the digital world?
- Is data protection the area that connects all the dots? What about consumer rights protection or competition?
- What role for private enforcement actions (e.g., via consumer and other civil society organisations) to drive change and ensure an interdisciplinary approach to enforcement?

13:00 - LUNCH

14:15 – COLLECTIVELY MAKING IT WORK: (F)LAWS OF INDIVIDUAL APPROACHES TO RESIST PLATFORM POWER

Organised by IViR, University of Amsterdam (NL)

Moderator Divij Joshi, University College London (UK)

Speakers Anton Ekker, Ekker Advocatuur (NL); Jill Toh, IViR, University of Amsterdam, (NL); Vanessa Barth, IG Metall, FairTube project (DE); Eike Gräf, European Commission (EU)

Existing approaches to regulating the political economy of data – and the power asymmetries they enable – fail to tackle many collective harms. The power and capital of tech companies is bolstered by the ways in which data-centric technologies intersect with labour. This has been increasingly evident in the context of gig work, whereby data and algorithmic management have been used to surveil, control and reorganise the workforce, resulting in tangible, systemic harms. While GDPR rights are increasingly used strategically to tackle these power asymmetries and render digital infrastructures more transparent, important questions remain as to their collective dimension. Moreover, recent policy developments aimed at addressing some of these unequal power dynamics rarely prioritise labour concerns and workers’ perspectives. This panel will explore the challenges faced *and* raised by regulatory initiatives, looking at on-the-ground efforts to better engage with the collective.

- What is the problem with data protection law discourse focusing on the individual rather than the collective? What are the practical challenges that manifest due to this individualisation of rights?
- What can the labour perspective bring to a better engagement with collective rights in the regulatory and governance debates on data and technology?
- How do some of the on-the-ground efforts illustrate ways of collectivising and what role do data (transparency) rights play in these wider efforts?

- How can current legislative efforts regulating technology (companies) better address collective harms?

15:30 - COFFEE BREAK

16:00 – DARK PATTERNS AND DATA-DRIVEN MANIPULATION

Academic ☆☆☆ **Business** ☆ **Policy** ☆

Organised by Leiden University (NL)

Moderator Mark R. Leiser, eLaw, Leiden University (NL)

Speakers Mireille Caruana, University of Malta (MT); Catalina Goanta, Maastricht University (NL); EgeyIn Braun, European Commission (EU); Agustin Reyna, BEUC (BE)

Lawmakers and regulators are increasingly expressing concerns about the rise and use of manipulative design techniques implemented into user interfaces across web pages, social media networks, apps, and platforms that trick and deceive users into an action that they would not have taken without the manipulative design. Collectively these are referred to as ‘dark patterns’, a term coined as ‘tricks used in websites and applications that make users do things that they did not mean to, like buying or signing up for something’. As dark patterns are deliberately designed to confound users or make it difficult or expensive for them to express their actual preferences, regulators in the United States and Europe have begun, not only raising their disapproval of, but introducing legislation to prevent their use and have even brought enforcement proceedings against major technology platforms accused of using dark patterns. This panel aims to discuss the role of consumer protection, in particular the Unfair Commercial Practices Directive and consumer protection enforcement for protecting users from all forms of data driven manipulation.

- Can consumer protection regulation mitigate the shortcomings of data protection law in dealing with dark patterns and data-driven manipulation?
- How can using evidence-led insights into how dark patterns manipulate behavior inform policy and rule makers?
- How will changes to the Unfair Commercial Practices Directive provide protection from dark patterns and data driven manipulation?
- Can consumer protection bridge the enforcement gap?

17:15 – MOBILITY DATA FOR THE COMMON GOOD? ON THE EU MOBILITY DATA SPACE AND THE DATA ACT

Academic ☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by Future of Privacy Forum (FPF) (US)

Moderator Rob van Eijk, Future of Privacy Forum (NL)

Speakers Laura Cerrato, Centre d’Informatique pour la Région de Bruxelles (BE); Arjan Kapteijn, Autoriteit Persoonsgegevens (NL); Maria Rosaria Coduti, DG CNECT (BE); David Wagner, FÖV (German Research Institute for Public Administration) (DE)

Sharing mobility data for the common good needs careful assessment because context matters. To what extent can citizens benefit from mobility data without having to sacrifice their rights and freedoms? In this panel we will dive into the upcoming EU Mobility Data Space, which is one of the ten data spaces proposed by the European Commission. Furthermore, we will explore how the Data Act may tap the potential of horizontal (cross-sector) data sharing, while empowering citizens to make better decisions and protect their privacy.

- How can the upcoming Data Act and EU Mobility Data Space address cities’ innovation and sustainability goals, while still safeguarding citizens’ privacy?
- Are current frameworks, such as the Mobility Data Sharing Agreement, covering stakeholders’ needs for legal certainty when sharing data for the common good?
- What are relevant use cases for privacy-preserving bolstered exchanges of data in this space?
- How to assess the cross-sharing of mobility data in context?
- Data minimisation concerns: can location data collected and shared by mobility service providers effectively be anonymised?

18:30 – COCKTAIL SPONSORED BY EPIC in Le Village

08:45 – UPLOAD_ERROR: AUTOMATED DECISIONS, USERS' RIGHT TO REDRESS, AND ACCESS TO JUSTICE ON SOCIAL NETWORKS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Amsterdam Law & Technology Institute, VU Amsterdam (NL)

Moderator Sarah Eskens, Amsterdam Law & Technology Institute, VU Amsterdam (NL)

Speakers David Martin Ruiz, BEUC (BE); Valentina Golunova, Maastricht University (NL); Andrea Baldrati, Privacy Network (IT); Silvia De Conca, Amsterdam Law & Technology Institute, VU Amsterdam (NL)

Social media continuously moderate content on their platforms. In doing so, they need to balance the freedom of expression rights of those who upload content with the interests of other individuals and groups to remove harmful content. Platforms like Facebook and Instagram currently mix automated and human decisions. Over- and under-inclusive interventions remain, however, a daily occurrence. Legitimate content is automatically taken down, harmful content sometimes remains online notwithstanding the reports of users. The GDPR provides a right not to be subject to automated decision-making but it is an open question if this right can provide redress with regard to content moderation. The new Digital Service Act introduces the right of redress for users. But what does it entail, and are there alternative solutions to explore? What are the limits of individual access to justice within privately owned online platforms?

- What is the role and what are the limitations of the redress tools against automated content moderation offered by the GDPR?
- What is the role and what are the limitations of the new right of redress introduced by the Digital Services Act against automated content moderation?
- Are there any alternatives to automated decisions implementing the T&S of a social media platform?
- Is there an “access to justice” right in the context of privately owned social media? What are its main elements?

10:00 – COFFEE BREAK

11:45 – POLICE: WE CAN'T STAND LOSING YOU - FORTNITE UNDERCOVER AVATARS ARE ONLY THE BEGINNING

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆

Organised by EDEN

Moderator Jan Ellermann, Europol (EU)

Speakers Véronique Bechu, Central Unit for Minor Victims (FR); Isabelle Debré, Association L'Enfant Bleu (FR); Fabrice Plazolles, Havas Play (FR); Gregory Mounier, Europol (EU)

What do a blue-winged angel and an online game have in common? They manifest that the future is already here to stay. The panel focuses on how innovation can contribute to making our world a safer place. For the first time, Europol awarded the Europol Excellence Award in Innovation during the annual European Police Chiefs Convention 2021. With this award, Europol aims to put in the spotlight the law enforcement community's most innovative initiatives and operations.

The Fortnite undercover avatar was an innovative tool to fight child abuse online (French Police Nationale), a creative approach based on the development of an online avatar in the video game Fortnite to which children could report if they were sexually harassed at home. After validation from the Central Unit for Minors Protection within the Central Directorate of the Judiciary Police, a team of 50 volunteers and psychologists connected to the game 14 hours a day, seven days a week from April to May 2020 to assist children asking for help. During this period, 1 200 children asked for help, out of which thirty percent were in a dire situation. Investigations were opened in a number of cases, and the children safeguarded.

Véronique Bechu, Isabelle Debré and Fabrice Plazolles talk about how law enforcement, an NGO and a private company joined forces to make Fortnite a safer (cyber)space where children reported sexual abuse and other forms of serious crime. Gregory Mounier will contribute with insights from Europol's Innovation Lab and its mission is to help the European law enforcement community to make the most of emerging technologies by developing innovative solutions to improve the ways in which they investigate, track and disrupt terrorist and criminal organizations and keep European citizens safe.

- Which risks emerge considering the fact that minors expose more and more personal data online?
- How can online games help law enforcement protect minors from sexual abuse and other forms of crime?

- How will policing work in the Metaverse?
- How can law enforcement agencies, civil society and private industries collaborate to protect vulnerable groups and what are the data protection related challenges?

13:00 – LUNCH

14:15 – RESEARCH AND BEST PRACTICE TO ADDRESS SOCIO-TECHNICAL RISKS IN AI SYSTEMS

Academic ☆☆ **Business** ☆☆ **Policy** ☆☆

Organised by Microsoft (US)

Moderator Slavina Ancheva, European Parliament (EU)

Speakers Michael A. Madaio, Microsoft Research (US); S.N.R. (Stefan) Buijsman, TU Delft (NL); Colin van Noordt, Tallinn University of Technology (EE)

Research and best practices in addressing risks in AI systems have significantly progressed over the last years. This panel looks at the most challenging problems and advances in research to support fairness, accountability, transparency and equity in AI. The panel will also examine whether the AI Act's requirements for trustworthiness will be flexible enough to address these objectives, nuanced enough to tackle the diversity of AI systems and their specific risks as well as the pace of innovation.

- Are the requirements able to tackle the socio-technical challenges of AI systems?
- What are the criteria against which the AI Act requirements will be measured?
- Are outcome-based goals an alternative?
- How can AI deployers be supported in their fairness work in practice?
- How can stakeholders impacted by AI participate in designing fairer and more responsible AI?

15:30 – COFFEE BREAK

16:00 – DATA PROTECTION CERTIFICATION – INTERNATIONAL PERSPECTIVE AND IMPACT

Academic ☆ **Business** ☆☆ **Policy** ☆☆☆

Organised by Mandat International, International Cooperation Foundation (INT)

Moderator Luca Bolognini, Italian Institute for Privacy (IT)

Speakers Peter Kimpian, Council of Europe (INT); Fabrice Naftalski, EY Avocats (FR); Sébastien Ziegler, European Centre for Certification and Privacy (LU); Chiara Romano, Italian Data Protection Authority (IT); Marcel Vogel, Federal Data Protection and Information Commissioner (CH)

The GDPR makes over 70 references to data processing certification in line with its art. 42, including for cross-border data transfers (Art. 46). Similar certification mechanisms are embedded in other data protection regulations. This session will provide an overview of the latest developments in data protection certification in Europe and internationally. The session will start by introducing the recent evolution of data protection certification. The Swiss Supervisory Authority (FDPIC) will present the experience and perspective of data protection certification in Switzerland based on many years of experience. The Council of Europe (CoE) will provide a complementary perspective on data protection certification at the international level. The European Centre for Certification and Privacy (ECCP) will present and discuss some innovative models in certifying the compliance of data processing under the GDPR and other regulations. The session will conclude by a panel discussion on expectations, challenges and opportunities with regards to international and mutual recognition of such certification.

- What are the lessons learned and opportunities with data protection certification?
- What is the potential for international recognition of data protection certification?
- What are the differences between universal, specific, and hybrid certification mechanisms? What are their benefits and disadvantages?
- What challenges organisations face following the adoption of the GDPR?
- What are the current state-of-the-art certification solutions for certifying and demonstrating GDPR compliance?

17:15 – DATA PROTECTION AS PRIVILEGE? DIGITALISATION, VULNERABILITY AND DATA SUBJECT RIGHTS

Academic ☆☆☆ **Policy** ☆☆☆☆

Organised by SPECTRE project (BE)

Moderator Jonas Breuer, SPECTRE (VUB)(BE)

Speakers Yigit Aydinalp, European Sex Workers Rights Alliance (EU); James Farrar, Worker Info Exchange (UK); Stefania Milan, University of Amsterdam (NL); Paola Pierri, Democratic Society (EU)

Vulnerable individuals and communities are impacted by a lack of digital literacy and e-inclusion in today's digitalized societies, which idealise the "tech-savvy, independent, and uber-modern, able to produce digital data and analyze it to hold city government accountable" as Burns and Andrucki (2020) argue. This panel revisits vulnerability, zooming in on the impacts of digital technologies. It discusses how new forms of vulnerability are created, or existing ones exacerbated, in societies informed through technologically mediated networks and ICT. Data subject rights may be promising tools as they aim to empower individuals and counter power asymmetries. The panel therefore looks into whether regulatory frameworks (data protection, administrative law) are mature and apt enough to tackle the challenge of protecting the rights and interests of those who find themselves increasingly marginalized while others reap the benefits of digitalisation. In this regard, the panel aims to ask the following questions:

- What are vulnerable data subjects, and what is the interplay of new and old vulnerabilities with increasing digitalisation in our society?
- Can data protection law, and especially the data subjects' rights, help vulnerable individuals to improve their position in society/ avoid exploitation?
- Have they been used in practice to counter vulnerabilities though, or are they a privilege, mainly at the hands of tech-savvy elites? What other, more collective tools, exist to address digitalisation's adverse and uneven impacts on certain groups?
- Faced with many problems in the offline world (poverty, literacy, socio-demographic background, inequalities, disenfranchisement and so on), how can vulnerable individuals as well as their representative organisations understand the impacts of digitalisation and act upon them?

18:30 – COCKTAIL SPONSORED BY EPIC in Le Village

CPDP2022 PANELS AT AREA 42 PETITE

08:45 – GOODBROTHER: PRIVACY, CORONAVIRUS, AND ASSISTED LIVING TECHNOLOGIES

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆

Organised by Cost Action 19121 'GoodBrother' (EU)

Moderator Liane Colonna, CA 19121 GoodBrother Member, Stockholm University (SE)

Speakers Carina Dantas, SHINE 2Europe/European Connected Health Alliance (PT); Birgit Morlion, European Commission (BE); Eduard Fosch-Villaronga, Leiden University (NL); Aleksandar Jevremovic, Singidunum University (RS)

More than 155 million people have recovered from Covid-19. However, the symptoms can last longer than expected. Remote patient monitoring with the use of speech and video technologies has proven to be an effective means to monitor the vital signs of frail people as well as healthy individuals who may be at risk of infection. The potential for wearable and wireless sensor technologies to reliably measure physiological parameters and habits of people appears to be great and likely to remain so even in the post-pandemic context.

On the other hand, since healthcare technology is increasingly integrated in private spheres and captures highly sensitive personal data, these developments may cause serious concerns about privacy and data protection. For this reason, a dialogue about the legal and ethical challenges in Active Assisted Living is necessary to develop widespread awareness on these topics.

- What are the ethical, legal, and privacy issues associated with audio- and video-based AAL technologies?
- What is the role of data protection law when it comes to safeguarding sensitive classes of data like race, age and gender collected by audio- and video-based sensors in the home?
- What privacy-by-design methodologies are available in order to protect the fundamental rights of those being monitored by audio- and video-based AAL technologies?
- How can we combine perspectives on privacy and data protection issues arising from the use of AAL technologies concerning healthcare automation?

10:00 - COFFEE BREAK

10:30 – RESPONSIBLE IoT IN PUBLIC SPACE - WHO IS ACTUALLY RESPONSIBLE FOR WHAT?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by University of Twente / Project BRIDE (NL)

Moderator Sage Cammers-Goodwin, University of Twente (NL)

Speakers Michael Nagenborg, University of Twente (NL); Sanna Lehtinen, Aalto University (FI); Alec Shuldiner, Autodesk (US); Valda Beizitere, DG JUST (EU); Erik Valgaeren, Stibbe (BE)

Smart city projects often include the use of sensors in public urban spaces. Thus, users of these spaces hardly have an opportunity to opt-out of these systems. In our panel, we will discuss the responsibilities of public and private actors regarding the development, placement and use of such systems beyond GDPR compliance. We will especially focus on the interface between municipalities and local authorities on the one side and private tech companies on the other side. How can municipalities, e.g., steer and govern technological developments? Should and can cities act on behalf of citizens and other city users? Is it sufficient to inform and educate citizens about data collections in public spaces? Or do cities do more?

- How to inform the public about sensors in public space?
- What options do local authorities have to steer technology development and deployment?
- Is it sufficient if technology developers follow the existing frameworks?
- How much room should there be for local differences?

11:45 – BIG BROTHER OUT TO LUNCH

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆☆

Organised by PROTEIN project (EU)

Moderator Eugenio Mantovani, VUB, LSTS (BE)

Speakers Tanja Schneider, University of St Gallen (CH); Maria Hassapidou, International Hellenic University and European Association for the Study of Obesity (GR/UK); Wolfgang Schmitt, European Consumer Organisation (BE); Olga Gkotsopoulou, VUB/HALL (BE)

Personalized nutrition technologies leverage on the collection and analysis of large volumes of data related to individuals' dietary behavioural patterns, physical activity and other parameters to provide generic and tailored nutrition, fitness and life-style advice. Till today there is no common definition as to what personalized nutrition entails. What there is agreement on is that it is a multifaceted concept of many levels and fragmented regulation. This panel discusses some of the impacts that such technologies have on private life. On one hand, the panel delves onto the concerns about the use of sensitive personal data, the surveillance one subjected to while eating, shopping for food, or doing sports, and the trustworthiness of applications marketed as well-being apps while impinging on health status. On the other, the panel draws attention to the blurred lines between lifestyle and health, health data and non-health data, medical and non-medical context - leading ultimately to questions of consumer safety, discrimination and stigma.

- How has our relationship to food and nutrition evolved over the years, both at an individual and a societal level?
- How 'personalised' is personalized nutrition in practice?
- What are the legal implications when widely available personalised nutrition products are consumed by the non-intended consumer or the non-intended consumer group?
- How does food law interact with data protection law?

13:00 - LUNCH

14:15 – PRIVACY DESIGN, DARK PATTERNS, AND SPECULATIVE DATA FUTURES

Academic ☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by SnT, University of Luxembourg (LU)

Moderator Cristiana Santos, University of Utrecht (NL)

Speakers Régis Chatellier, CNIL (FR); Stefano Leucci, EDPS (EU); Dusan Pavlovic, White Label Consultancy (NO/PL); Arianna Rossi, SnT, University of Luxembourg (LU); Cennydd Bowles, NowNext (UK)

Opposite forces harshly confront each other on the battlefield of digital services. On one side, privacy-invasive mechanisms like dark patterns pervert the fairness that should govern personal data use. Neither legislation nor slow-paced case law seems able to counteract the pervasiveness and impact of online manipulation.

On the other side, the harm caused by malicious designs is increasingly being exposed and a growing number of transparency-enhancing technologies is being created to support the rights of data subjects.

But we can only devise and implement overarching data protection by design if we become able to anticipate trends, explore the future implications of technology and guide its development towards desirable outcomes. In the end, which brighter worlds do we intend to design to ensure fair, transparent, human-centred use of personal data?

- How are businesses, academics and regulatory bodies currently mitigating dark patterns?
- What kind of transparency mechanisms should be further designed?
- How might we anticipate emerging trends to prevent risks and drive the development of data-driven services?
- How might law, human-centred design and foresight work together to breed trust in digital services and fight online manipulation?

15:30 - COFFEE BREAK

16:00 – EDPL YOUNG SCHOLAR AWARD

Academic ☆☆☆☆☆☆

Organised by EDPL Young Scholar Award

Moderators Bart van der Sloot, Tilburg University (NL), Wolfgang Andreae, Lexxion Publisher (DE)

Up-and-coming data protection researchers compete every year for the prestigious Young Scholars Award (YSA) organised by the European Data Protection Law Review (EDPL).

The best 3 young authors are invited to present their research at the YSA panel.

- Yannick Alexander Vogel, Università di Bologna (IT) - Stretching the Limit, The Functioning of the GDPR's Notion of Consent in the context of Data Intermediary Services
- Felix Zopf, Universität Wien (AT) - Two Worlds Colliding – The GDPR in Between Public and Private Law
- Brooke Razor, Faegre Drinker (UK) - Examining Obligations of EU States to Address the Gender Data Gap

The papers will be discussed with the selection jury of renowned experts: Gloria González Fuster, Vrije Universiteit Brussel (BE), Hielke Hijmans, Vrije Universiteit Brussel (BE), Alessandro Spina, European Commission, Franziska Boehm, FIZ Karlsruhe – Leibniz Institute for Information Infrastructures (DE).

At the end of the panel, the winner of the 6th EDPL Young Scholar Award will be revealed and receive the prize.

17:15 – TECHNOLOGY AND POWER IN TIMES OF CRISIS

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆☆

Organised by Global Data Justice project, Tilburg University (NL)

Moderator Aaron Martin, TILT (NL)

Speakers Grace Mutung'u, CIPIT (KE); Mariana Rielli, Data Privacy, (BR); Frederike Kaltheuner, Human Rights Watch (US); Ian Brown, Fundacao Getulio Vargas (BR)

This panel will examine how new markets and opportunities opened up by the Covid-19 pandemic have shaped business strategies for technology firms in the EU and worldwide. Technology firms are increasing their markets in public health logistics (contact tracing, vaccine certification, information distribution), educational technology and many other areas thanks to the pandemic. Less visibly, there is huge growth in the market for ID and biometric technologies, bordering technologies and home-working surveillance applications. These shifts have been accompanied by decreased controls on competition and an increased tendency on the part of authorities to legitimise pandemic-related innovation even when it challenges established boundaries. The panel will discuss the implications of these power shifts for regulators and advocacy organisations, comparing different regional challenges and possible policy and regulatory responses in the areas of privacy, data protection, competition regulation and civil society action.

- How has the emergency of the pandemic reshaped markets for technology firms?
- What new challenges does the pandemic create for policymakers, regulators and advocacy organisations interested in digital justice and rights?
- Do pandemic-related shifts in technological power differ across regions?
- How should regulatory and civil society power balance these shifts in market share and commercial infrastructure?

18:30 – COCKTAIL SPONSORED BY EPIC in Le Village

07:30 - Registration in La Cave
08.15 - Welcome coffee in Le Village

CPDP2022 PANELS AT GRANDE HALLE

08:45 – CAN LAW BE DETERMINATE IN AN INDETERMINATE WORLD?

Academic ☆☆☆☆☆☆
Organised by CDSL
Moderator Vagelis Papakonstantinou, CDSL-VUB (BE)
Speakers Indra Spiecker gen. Döhmman, Goethe University (DE); Giovanni Sartor, EUI (IT); Sophie Stalla-Bourdillon, University of Southampton (UK); Dara Hallinan, FIZ Karlsruhe – Leibniz Institute for Information Infrastructures (DE)

Over the past decades, advances in information processing have produced societies of increasing complexity and indeterminacy – at least under some interpretations. Presuming a link between legal systems and the societies of which they are a part, we might presume that increases in social complexity and indeterminacy will also have an impact on legal systems – both on their substantive content and on the structures which provide and maintain this content. Further presuming that legal systems exist to provide a degree of certainty to the structuring of social relations, we arrive at a more concrete question: How can law remain determinate in an increasingly indeterminate world. This panel sets out with the ambitious task of providing some insight in relation to this question, and will consider issues such as:

- How might we understand the idea of indeterminacy?
- What are the pressures placed on legal systems by indeterminacy?
- What are the limitations in the ability of legal systems to respond to these pressures?
- Do we already see paradigms emerging in response to these pressures?

10:00 - COFFEE BREAK

10:30 – PRACTICAL PERSPECTIVES ON INTERNATIONAL TRANSFERS

Business ☆☆☆☆ **Policy** ☆☆
Organised by CPDP
Moderator Laura Linkomies, Privacy Laws and Business (UK)
Speakers Diletta De Cicco, Steptoe (BE); Ruth Boardman, Bird & Bird (UK); Laura Brodahl, Wilson Sonsini Goodrich & Rosati (BE); Ludmila Georgieva, Google (BE)

There remains considerable uncertainty as to how international transfers of personal data under the GDPR should be legitimated. Data controllers and processors in the EU are often left in a state of confusion as to whether, and how, they might engage in international transfers. Questions swirl concerning, for example, which approaches might be used in relation to which countries, as to the degree to which evaluations of national laws in third countries should be carried out, and as to how the situation may change in future. Against this background, this panel brings together practicing lawyers and policy professionals who deal with the legitimation of international transfers under the GDPR on a daily basis. Panelists will offer their perspectives on the current situation and will consider, amongst others, the following questions:

- What are the best ways to legitimate international transfers, and why?
- What novel approaches have come to the fore in dealing with international transfers over the past couple of years?
- How should lawyers and other professionals deal with the ongoing uncertainty surrounding the legitimation of international transfers?
- What can legal practice tell us about policy solutions moving forwards?

11:45 – INTERNATIONAL TRANSFERS ON THE GROUND

Business ☆☆☆ **Policy** ☆☆☆
Organised by CPDP
Moderator Laura Drechsler, VUB (BE)
Speakers Eduardo Ustaran, Hogan Lovells (UK); Christian Brundell, Squire Patton Boggs (UK); Alan Butler, EPIC (US); Aaron Cooper, BSA | The Software Alliance (BE); Alisa Vekeman, DG Just (EU)

Following the previous panel, this panel continues the theme of the practical issues surrounding international transfers under the GDPR. This panel takes a broader perspective and considers the real-world impact of the law surrounding international transfers, and efforts on the ground to approach these issues. With this in mind, this panel brings together speakers from different sectors and with different perspectives. Panelists will consider, amongst others, the following questions:

- What are the different types of impacts - for example on companies and individuals - from current law on international transfers?
- What changes have recent developments in law - for example in Schrems II - produced on the ground? ·
- What steps are being taken, by practitioners, policy makers, etc. to tackle those changes?·
- In light of the current situation, what needs to be done moving forward?

13:00 - LUNCH

14:15 – WILL THE DIGITAL EVER BE NON-BINARY?
THE FUTURE OF TRANS (DATA) RIGHTS

Academic ☆☆☆ **Business** ☆ **Policy** ☆☆
Organised by CPDP
Moderator Gloria González Fuster, Law, Science, Technology & Society (LSTS), VUB (BE)
Speakers Jens Theilen, Helmut-Schmidt-University in Hamburg (DE); Alex Hanna, Distributed AI Research Institute (US); Kevin Guyan, School of Culture and Creative Arts at the University of Glasgow (UK); Kirstie English, University of Glasgow (UK)

In a world that increasingly recognises that gender cannot be understood as binary and immutable, technology and law appear to be still too often trapped in male/female classifications, leaving aside the rights, needs and concerns of those who are un- or mis-represented by such classifying canvas, and possibly harmed by it. And in a Europe lacking a consistent approach towards the recognition of gender identities, the debate on how to appropriately protect gender identifies online is far from being solved. This panel will discuss privacy and data protection rights of non-binary and trans individuals, but also deeply intertwined issues around data collection and (legal and technical) gender categorisation. Aiming at throwing light on how to best protect the digital rights of all, which necessarily requires taking seriously the digital rights of LGBTQ+ individuals, it will ask:

- How to protect better the data rights of non-binary and trans communities?
- Do we need less data, more data, and/or different data?
- Which role for law and which role for technology in this process of rethinking gender categorisation practices?
- And what can we learn for a better (data) protection of all, regardless of their gender?

15:30 - COFFEE BREAK

16:00 – TRUST & TRANSPARENCY IN AI: DISCUSSING HOW TO UNPACK THE
“BLACK BOX”

Academic ☆☆☆ **Policy** ☆☆☆
Organised by Uber (US)
Moderator Simon Hania, Uber (NL)
Speakers Ivana Bartoletti, Women Leading in AI (IT/UK); Diana Calderon Medellin, DeliveryHero (DE); Guido Scorza, DPA (IT); Gabriele Mazzini, DG CNECT (EU)

The future of AI is here and already seamlessly integrated into a variety of sectors, from healthcare to transportation. Despite AI becoming more ubiquitous, surveys indicate that trust in AI continues to be low, especially among individuals in the U.S. and EU. Much of this seems to stem from fundamental misunderstanding about what artificial intelligence and machine learning are. However, improving transparency in AI on an ongoing basis can be a “moving target,” with hundreds of definitions and new findings that promote responsible AI development, deployment, and integration. Join us for a conversation about what meaningful transparency in AI practically looks like and how organisations should prepare for GDPR-like rules for AI governance.

- What does “transparency” mean in the context of AI, what are the target groups and why is it beneficial?
- Is there a need to understand in detail how AI works or rather the positive or negative effects it can produce based on its input?
- What obligations or incentives should be put in place, how, when and on whom?
- How can we effectively demonstrate and verify that obligations are fulfilled and incentives used?

17:15 – WHY PRIVACY MATTERS AND THE FUTURE OF DATA PROTECTION LAW

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Cordell Institute, Washington University (US)
Moderator Helen X. Dixon, Data Protection Commissioner of Ireland (IR)
Speakers Frederik Zuiderveen Borgesius, Radboud University (NL); Natali Helberger, University of Amsterdam (NL); Mireille Hildebrandt, VUB (BE); Neil Richards, Washington University (US)

Data protection laws are currently spreading across the globe, but they are often proposed and enacted without much consideration of their definitions of privacy and the human values that they support. A complete consideration of “data protection and privacy in transitional times” requires us to reconsider why privacy and data protection rules exist, what values they serve, and what they should look like in the future. This panel brings together leading European and American academic and regulatory experts to ask these hard and essential questions of privacy and data protection law. Using the argument in Neil Richards’ recently published Why Privacy Matters (OUP 2022) as an initial starting point, the panel (and audience) will discuss the big questions of what privacy and data protection law is, what it is trying to achieve, and where it falls short.

- Why do privacy and data protection matter? What values do they serve?
- What is the relationship between privacy and data protection rules and identity formation, political freedom, and consumer protection?
- How should our understandings of privacy and data protection change as we confront new problems like public health emergencies, artificial intelligence, and pervasive data collection and computing?
- Is a shared understanding of what privacy is and why it matters possible across the different legal systems on both sides of the Atlantic?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS)

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON in Le Village

CPDP2022 PANELS AT LA CAVE

08:45 – PERSONAL DATA IN TEXTS: DETECTION, ANNOTATION AND GOVERNANCE

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Université de Bourgogne Franche-Comté (UBFC) (FR)
Moderator Iana Atanassova, Université de Bourgogne Franche-Comté (UBFC) (FR)
Speakers Thierry Bregnard, Haute École de Gestion Arc/HEG-Arc (CH); Walid El Abed, Global Data Excellence (CH); Sylviane Cardey, Université de Bourgogne Franche-Comté/UBFC (FR); Hitoshi Isahara, Otomon Gakuin University (JP)

The new GDPR regulation requires that any company must be able to prove that the personal data it holds are protected and, above all, unusable in case of theft. This has created a new need for automatic tools to identify and mask protected data, including in texts, in order to facilitate companies’ compliance with the legislation. The creation of such tools, that allow robust and versatile text processing to handle personal data, is still an important issue and requires the creation of specific semantic models for linguistic AI. This panel will outline the current landscape in the processing of personal data in texts, by providing the point of view of both researchers in Natural Language Processing (NLP) and actors of the private sector. It will also address the question of data governance related to personal data in texts.

- What are the real needs of business when it comes to personal data processing for GDPR compliance?
- What is the role of personal data governance for the creation of value?
- How to create linguistic models for the processing of personal data?
- What algorithms do we need for the efficient processing of personal data in texts?

10:00 - COFFEE BREAK

10:30 – DIGITAL AGE OF CONSENT: LOOKING FOR A NEW PARADIGM

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by CEU San Pablo University (ES) - South EU Google Data Governance Chair (EU)
Moderator José Luis Piñar Mañas, CEU San Pablo University (ES)
Speakers Maria da Graça Canto Moniz, Nova University Lisbon (PT); Georgios Yannopoulos, National and Kapodistrian University of Athens (GR); Emma Day, Freelance Human Rights Lawyer (PT); Vincenzo Zeno-Zencovich, RomaTre University (IT)

One of the most important issues regarding children’s online privacy is to determine how to comply with the relevant provisions in Article 8 GDPR on parental consent. In this context, when the child is below the age of digital consent, the personal data processing will be lawful only if the consent is given or authorised by the person holding the parental responsibility over the child. We can identify an increasing number of ways to prove the children’s age online, using different methods and technologies. However, there are many issues to consider regarding the reasonable efforts that any controller should make to verify the validity of a child’s digital consent. In addition, it is essential to identify the dimension of the scope of the mention made by the European legislator regarding the available technological solutions allowing the said verification to be carried out. In this panel we will focus on several issues that will help define the scope of the obligations that the GDPR establishes for the different Internet operators:

- How the principles of privacy by design, privacy by default and data minimisation will play a role to effectively protect children?
- How should the different Internet operators face the challenge of protecting the interests of minors on the Internet and comply with the obligations that the GDPR establishes in relation to digital consent?
- What factors should be assessed to identify the most appropriate age verification methods?
- How to evaluate the adequacy of the means to be used in each context to express digital consent?

11:45 – TRANSITIONAL (LEGAL) TIMES FOR R&D AND R&I SECTORS

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by VALKYRIES H2020 Project - LIDER Lab Scuola Sant’Anna - Ethical Legal Unit (IT)
Moderator Denise Amram, Scuola Superiore Sant’Anna Pisa (IT)
Speakers Rowena Rodrigues, Trilateral Research (UK); Andrea Parziale, EURAC Research Italy (IT); Owe Langfeldt, DG JUST (EU); Pedro Ramon Y Cajal, INDRA (ES)

R&D and R&I sectors are currently affected by the European Strategy of Data as well as by the entering into application of EU legislative initiatives (Clinical Trials and Medical Device Regulations) and their balance with the ongoing debate on AI Regulation. The panel explores how the standardization and compliance processes will deal with the challenges and new obligations emerging by the uncertainties of the applicable ethical-legal framework in order to understand the possible domino effect produced by the GDPR towards the following EU initiatives aiming to enhance fundamental rights in the new technologies. Specific scenarios, investigated under the H2020 - VALKYRIES project as well (GA 101020676), will be discussed by the speakers, such as the development of AI solutions for first aid and multi-victim disasters, where health-related data are processed.

- Which are the most significant obligations for R&D and R&I emerging from the EU Strategy of Data framework and the already approved CTR, MDR, GDPR?
- What are the challenges in terms of standardization and compliance?
- How the proposal of AI Regulation will impact on the development of solutions
- Which specific safeguards shall be implemented in case of solutions processing health-related data for emergencies management?

13:00 - LUNCH

14:15 – ROLE OF ETHICS COMMITTEES IN THE EUROPEAN HEALTH DATA SPACE

Academic☆☆Business☆Policy☆☆☆
Organised by Standing Committee of European Doctors (CPME) (BE)
Moderator Sjaak Nouwt, KNMG (NL)
Speakers Guillaume Byk, DG SANTE (EU); Annika Eberstein, COCIR (BE); Otmar Kloiber, WMA (INT); Mélodie Bernaux, French Ministry of Health (FR)

The European Commission is expected to adopt a proposal for a Regulation on the European Health Data Space (EHDS) in the first quarter of 2022. Personal data collected from primary care via the electronic health records could be linked to the EHDS system in order to be used for health research purposes and policy-making. This repurposing activity will be based on the data subject’s consent but might also be based on another legal basis, such as the performance of a task carried out in the public interest or a specific Union law considering the further processing as compatible and lawful. When consent is not the legal basis, and data are identifiable, the EHDS should foresee greater involvement of ethics committees. The same reasoning should exist for the establishment of databases concerning health used for research and policy-making. This panel will take a deep dive on what specific countries are doing in this area and discuss possible recommendations on how, where and when in the procedure ethic committees could be involved in the EHDS (e.g. one-stop-shop).

- How can the EHDS support the use of clinical data and public health data for health research and policy decision-making while protecting patients’ privacy? What does the EHDS proposal foresee?
- How can the ethical principles for digital health developed by the French Presidency provide protection in the context of the EHDS? What is being done at national level and what is the interplay with data protection authorities?
- What role should ethics committees play today in relation to personal data concerning health? Should their role to change in relation to the EHDS? Should they have enforcement powers?
- Why does it matter to consider the Declarations of Taipei and Helsinki of the World Medical Association for the EHDS?

15:30 - COFFEE BREAK

16:00 – DATA PROTECTION NEW FRONTIERS IN BRICS COUNTRIES

Academic☆☆Business☆☆Policy☆☆
Organised by Center for Technology and Society at FGV/ CyberBRICS Project (BR)
Moderator Luca Belli, Center for Technology and Society at FGV Law School (BR/IT)
Speakers Danilo Doneda, National Council for Privacy and Data Protection (BR); Smriti Parsheera, CyberBRICS (IN); Sofia Chang, Center for Technology and Society at FGV (BR); Sizwe Snail, Information Regulator (ZA); Andrey Schcherbovich, CyberBRICS (RU)

The evolution of data protection regulatory frameworks in the BRICS Countries (Brazil, Russia, India, China, South Africa) has been quick and consistent, and is increasingly contributing to forge international standards as well as to broaden the frontiers of data protection regulation. This panel proposes do delve into new developments and common grounds among these new frameworks, considering, for example, the new Chinese data protection law, the first year of the Brazilian LGPD, the Indian data protection Bill, the Russian Internet Sovereignty debate, and the enforcement challenges in South African.

- What major developments took place in the BRICS data protection frameworks over the past year?
- How are BRICS countries innovating data protection policy and institutional frameworks?

- Digital sovereignty and cybersecurity are playing and increasingly important role in BRICS data protection circles. Can we identify common trends?

17:15 – SYNTHETIC DATA MEET THE GDPR: OPPORTUNITIES AND CHALLENGES FOR SCIENTIFIC RESEARCH AND AI

Academic☆☆Business☆☆Policy☆☆
Organised by University of Turin, UNITO (IT)
Moderator Eleonora Bassi, Nexa POLITO (IT)
Speakers Theresa Stadler, EPFL (CH); Massimo Attoresi, EDPS (BE); Pompeu Casanovas, La Trobe University Law School (AU); Jerome Bellegarda, Apple (US)

Huge amounts of personal data are increasingly collected by governments and the private sector. Such data are potentially highly valuable for scientists, e.g. for work on precision medicine and digital health. Striking a balance between free availability of data for research purposes and the protection of individuals from potentially harmful disclosure and misuse of information, however, is not an easy task. Efforts to guarantee effective de-identification methods have been so far inconclusive, particularly in the context of large datasets where it is extremely difficult to prevent re-identification of individuals. Synthetic data can capture many of the complexities of the original datasets, such as distributions, non-linear relationships, and noise. Yet, synthetic datasets do not actually include any personal data. We may provide solutions for well understood domains, augment domain data when acquiring such data is sensitive or expensive, and explore machine learning algorithms and solutions when actual domain data is not available. A number of opportunities and challenges follow as a result in the fields of artificial intelligence, e.g. machine learning applications, and personal data processing for scientific purposes, e.g. the re-use of personal data.

- How do synthetic data improve today’s state-of-the-art in AI?
- How can synthetic data improve today’s legal regulations on the processing of personal data for scientific purposes?
- What are the limits, e.g. translational or operative boundaries, of this approach?
- What personal data applications could be a game-changer through the use of synthetic data?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS) in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON in Le Village

CPDP2022 PANELS AT AREA 42 GRAND

08:45 – FROM SHAREHOLDER VALUE TO SOCIAL VALUE

Academic☆☆Business☆☆Policy☆☆
Organised by IEEE (AT)
Moderator Adriana Nugter, Vrije Universiteit Amsterdam (NL)
Speakers Sarah Spiekermann, Wirtschaftsuniversität Wien (AT); Ulrich Weinberg, Global Design Thinking Alliance (DE); Salvatore Scalzo, DG CNECT (EU); Lohan Spies, Sovrin Steward Council (SA); Alexandra Ebert, MOSTLY AI (AT)

The proposed EU AI Act highlighted the need for standards that support ethical alignment of applications. The IEEE7000 standard proposes concrete processes to build systems that bear a whole spectrum of social values. First case studies give hope that the standards’ processes deliver what was promised: to go from shareholder value to social value. But are companies ready to follow such a process framework? Is the positive vision of ‘technology for humanity’ realistic in times of global competition on cost and technological sovereignty; times where personal data market models and the attention economy seem to be firmly established? Is thorough planning and documentation, as well as good control over eco-system partners in contradiction with the current mantra of agile system development? Do we need a general return to ‘risk-thinking’ for any kind of system development?

- Is corporate strategy willing to sacrifice profit margins for human values?
- Are engineers ready to forgo some agility for the sake of value-based requirements engineering and transparent system design (which implies documentation)?
- Is it realistic to establish and live strong eco-system control?
- Do we really need risk-based design approaches only for high-risk applications?

10:00 - COFFEE BREAK

10:30 – TACKLING SURVEILLANCE AND ITS BUSINESS MODEL THROUGH DECENTRALISATION - DISCUSSING INFRASTRUCTURE AND TOKEN ECONOMICS

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆

Organised by Nym Technologies (CH)

Moderator Claudia Diaz, Nym and KU Leuven (BE)

Speakers Renata Avila, Open Knowledge Foundation (GT); Jaya Klara Brekke, Nym Tech, Weizenbaum Institute, (DE/UK); Carissa Véliz, Oxford (UK); Chelsea Manning, Nym (INT)

In the context of mass-surveillance, traffic analysis and Machine Learning, privacy cannot be a question of individual preference. But how can we make privacy the default and build a global privacy infrastructure, in practice? Current internet business models are all about collecting and exploiting data. With centralised parties running the infrastructure, user consent is a joke. “Take it or leave it” is not a meaningful choice for basic infrastructure. COVID-19 is set to exacerbate this, with more processes going digital, and the roll-out of contact tracing and vaccine certificates. In reaction to centralisation and data exploitation, recent years have seen a wave of decentralised technologies. New protocols, blockchains, DLTs and DAOs aim to challenge surveillance capitalism by proposing new models for the internet. This panel will discuss these as an infrastructural approach, and how it can further the aim of global privacy.

- Can we have a decentralised approach to privacy-preserving infrastructures that removes the big powerful providers that collect data for profit?
- How can we ensure all participants have the right incentives to make the system sustainable?
- By decentralising privacy infrastructure, can we remove the surveillance incentive?
- In such a decentralised infrastructure, who is trusted for what?

11:45 – POWER OVER DATA AND ALGORITHMS: CAN WE GET IT BACK?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by Ada Lovelace Institute (UK)

Moderator Ravi Naik, AWO (UK)

Speakers Paul Nemitz, European Commission (EU); Katarzyna Szymielewicz, Panoptykon Foundation (PL); Michael Veale, University College London (UK); Raegan MacDonald, Mozilla (US)

Today’s complex but invisible data infrastructures, operated and controlled by dominant tech platforms, block the way for more sustainable, privacy-protective and user-centric business models that place emphasis on accountability towards individual users and are mindful of the social impacts. The panel will discuss what regulatory, technological and institutional transformations are needed in order to reclaim the power over data and algorithms from dominant platforms and re-channel it to serve individual and societal goals. Invited experts will discuss the most promising avenues, which include data sharing structures and governance models, and new types of infrastructure and institutions that could emerge following the European data strategy. The panel will acknowledge risks and practical difficulties that come with potential transformations that aim to change how power over data and algorithms operates. These changes can be opening up the core functions of dominant platforms via interoperability measures, opening access to data controlled by dominant platforms for non-commercial purposes and introducing data governance intermediaries motivated by social goals. These insights will be based on preliminary findings made by the Rethinking Data working group set up by the Ada Lovelace Institute.

- How do the proposed measures in the European data strategy (which includes the Data Governance Act, Digital Markets Act, Data Act) meet the ambition to re-channel the use of data and algorithms towards societal goals? Are these measures fit for purpose?

- What data protection and data security safeguards need to be built in the design of new data governance frameworks, institutions and infrastructures to prevent loopholes, harms and abuses?
- What would new power structures and a new role for data look like, beyond what has been proposed in the Data Governance Act and the Data Act, to address structural dependencies and strengthen accountability?

13:00 - LUNCH

14:15 – IS A EUROPEAN DATA STRATEGY WITHOUT TRADE-OFFS BETWEEN ECONOMIC EFFICIENCY AND FUNDAMENTAL RIGHTS PROTECTION POSSIBLE?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by Open Future Foundation (NL)

Moderator Balázs Bodo, IViR (NL)

Speakers Heleen Janssen IViR (NL) and Computer Science & Technology, University of Cambridge (UK); Alek Tarkowski, Open Future Foundation (NL); Damian Boeselager, European Parliament (EU); Lorelein Hoet, Microsoft (BE)

European data strategy and its key legislative measures, the Data Governance Act and the Data Act, have two stated goals. First, the strategy seeks to grow the data economy, innovation and data use in the Single Market. Second, a citizen-centric commitment to European values is declared. These are potentially conflicting goals, as human rights protection is often seen as a barrier to economic growth. EU’s strategy introduces novel data governance models, including data cooperatives, enabling European data policies that support democratic, citizen-centric data governance. Meanwhile, these new governance models might, if interests involved are not robustly regulated, rather create risks to human rights, than help protect and foster these. Reconciling internal market interests while protecting European values is key, if Europe wants to achieve digital sovereignty, while forging a real and trustworthy alternative model to other emerging digital societies.

- Which policy measures in the new Data Strategy have greatest transformative potential for the Internal Market?
- What are the greatest expected drivers and obstacles of data-driven innovation within the European data strategy?
- What are the potential points of conflict between economic growth from data and fundamental rights within the European data governance framework?
- Can the European commitment to citizen-centric, democratic data governance be maintained under the perceived competitive pressure with China and the US?

15:30 - COFFEE BREAK

16:00 – LIMITS OF EMERGENCY POWERS: PROTECTING PRIVACY IN EXCEPTIONAL CIRCUMSTANCES

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆

Organised by EPIC (US)

Moderator Calli Schroeder, EPIC (US)

Speakers Kristina Irion, Institute for Information Law, University of Amsterdam (NL); Malavika Jayaram, Digital Asia Hub (IN); Rafael Zanatta, Data Privacy Brasil (BR); Patrick Penninckx, Council of Europe (INT)

The COVID-19 crisis has highlighted the need for strong data protection standards during public health emergencies. Governments and private entities have used contact tracing technologies, employee monitoring, surveillance drones, facial recognition, and more in an attempt to combat the spread of COVID, justified by a “state of emergency.” Italy, for example, approved the use of drones to surveil lockdown-violators during the pandemic, identify infected individuals, and even yell at offenders through recorded warnings.

Under many global legal regimes, certain rights may be curtailed or temporarily limited during states of emergency, exceptional circumstances, or due to pressing national interest. However, privacy advocates have been vocal about the need to ensure that emergency measures are limited – both in time and scope – and do not permanently undermine individual privacy rights or become the “new normal.”

- What limitations – both in law and in practice – currently exist on curtailing privacy protections during a state of emergency?

- How are privacy protections safeguarded by data protection authorities, civil rights groups, and others during a declared state of emergency?
- Are there areas that you believe most urgently require protections against exploitation during a state of emergency?
- How can we effectively combat potential abuse of “state of emergency” to curtail privacy rights?

17:15 – WHEN PRIVACY AND DATA PROTECTION RULES, WHAT AND WHO LOSES OUT?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Interdisciplinary Hub for Digitalisation and Society (iHub), Radboud University Nijmegen (NL)
Moderator Sarah Eskens, ALTI, Vrije Universiteit Amsterdam (NL)
Speakers Lee Bygrave, University of Oslo (DK); Augustin Reyna, BEUC(EU); Gloria González Fuster, Vrije Universiteit Brussel (BE); Tamar Sharon, iHub, Radboud University Nijmegen (NL)

When it comes to digital harms, privacy and data protection concerns have come to dominate public debate and regulation. While useful early on in the stride against the new power asymmetries of the digital era, the focus on privacy and data protection is currently engendering detrimental effects. Amongst others, the hegemony of the value of privacy may crowd out other values that are no less important or at risk in digital society – such as solidarity, democratic control and justice – or narrowly redefine them as privacy concerns. The focus on data protection may also be counterproductive at a time when Big Tech is developing privacy-friendly ways to expand into new sectors of society. Moreover, governments may increasingly use privacy to evade discussion and critique. The panel will address the effects of the rise to dominance of privacy and data protection concerns.

- What kind of strategic uses is privacy being put to, by corporations and governments?
- Where does data protection law fall short in protecting people from digital harms?
- Which values and rights have suffered from the focus on privacy and data protection, and deserve more attention?
- How can we explain the historical rise to dominance of privacy and data protection in public debate and regulation?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS) in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON in Le Village

CPDP2022 PANELS AT AREA 42 MIDI

08:45 – PIMS BUILDING THE NEXT GENERATION PERSONAL DATA PLATFORMS, A HUMAN-CENTRIC APPROACH

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Internet Users Association
Moderator Marco Mellia, Politecnico di Torino (IT)
Speakers Leonardo Cervera-Navas, EDPS (EU); Rodrigo Irarrazaval, WIBSON (ES); Paula Ortiz, IAB Spain (ES); Nikolaos Laoutaris, IMDEA (ES)

The Personal Information Management Systems (PIMS) concept offers a new approach in which individuals are the “holders” of their own personal information. PIMS allow individuals to manage their personal data in secure, local or online storage systems and share them when and with whom they choose. Individuals would be able to decide what services can use their data, and what third parties can share them. This allows for a human centric approach to personal data and to new business models, protecting against unlawful tracking and profiling techniques that aim at circumventing key data protection principles.

PIMS promises to offer not only a new technical architecture and organisation for data management, but also trust frameworks and, as a result, alternative business models for collecting and processing personal data, in a manner more

respectful of European data protection law. This panel will address PIMs from the perspective of the EU regulatory framework, new business models, tools for implementation and success stories. It will be of special interest for companies, developers and entrepreneurs interested in business proposals based on the personal data of European citizens.

- What are the benefits of data sharing for citizens?
- What is Europe's personal data strategy in both regulatory and business development?
- Are user-centric data models competitive?
- What are the main barriers to personal data-driven business development and how to overcome them?

10:00 - COFFEE BREAK

10:30 – MEASURING FUNDAMENTAL RIGHTS COMPLIANCE THROUGH CRIMINAL JUSTICE STATISTICS

Academic ☆☆☆ **Policy** ☆☆☆
Organised by MATIS project (BE)
Moderator Teresa Quintel, Maastricht University (NL)
Speakers Daan Vertongen, Belgian Passenger Information Unit (BE); Marianne Junger, Twente University (NL); Alexander Seger, Council of Europe (INT); Michael Levi, Cardiff University (UK)

The European legislators are rapidly developing digital investigation powers of law enforcement authorities, for example the access to Passenger Name Records or the cross-border access to electronic evidence. On the other hand, the cornerstone of the Digital Single Market are new, strong and robust data protection rules, designed to strengthen the protection of fundamental rights of individuals in the Digital Age.

These competing legislative developments are often implemented without objective evidence, which would justify their *raison d'être*. This panel should therefore explore whether we can empirically measure the use and frequency of digital investigation powers, and, based on such measurements, learn something about their fundamental rights compliance.

- What can we learn from the criminal justice statistics?
- Can we objectify the debate about the necessity and proportionality of digital investigation powers?
- Can we quantify the necessity test? What about proportionality?
- How do we ensure the tracing of the entire life cycle of personal data in the criminal justice system, from the moment of its collection/access until the end of the investigation/trial/sentencing?

11:45 – BOOK SESSION: ‘INDUSTRY UNBOUND’ BY ARI WALDMAN

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by CPDP and the Chair ‘Fundamental Rights and the Digital Transformation’ at VUB (BE)
Moderator Joris van Hoboken, UvA, VUB (BE)
Speaker Ari Ezra Waldman, Center for Law, Information and Creativity (CLIC), Northeastern University (US)
Discussants Rowenna Fielding, Miss IG Geek (UK); Svetlana Yakovleva, Institute for Information law, UvA, De Brauw Blackstone Westbroek (NL/BE)

In his book ‘Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power’, Ari Waldman shows how tech companies undermine privacy protections in practice. Building on years of research and interviews with privacy lawyers and professionals, his book reveals the layers of the tech industry’s stranglehold over privacy regulation. By dominating discourse, compliance, and design, the tech industry has managed to stack the cards against us and so effectively co-opt the privacy profession such that even those who call themselves privacy advocates on the inside do not realize how they are complicit in oppressive data extraction. In this special CPDP session, the author will provide an introduction to his book, and engage in a discussion with leading experts about the lessons and insights they draw from this insightful contribution to the field.

- What are the mechanisms through which corporate interests can dominate privacy work?
- What is the relevance of discourse and are there differences between Europe and the U.S. in this regard?
- Do we need more evidence in relation to privacy practices in Europe and the GDPR?
- In what way can privacy practices be made more meaningful in protecting privacy?

13:00 - LUNCH

14:15 – FALSE PRIVACY IN SHEEP’S CLOTHING: HARMFUL PATTERNS IN RECENT “PRIVACY” PROPOSALS

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Brave
Moderator Daragh Ó Briain, Castlebride (IE)
Speakers Pete Snyder, Brave (US); Maneesha Mithal, Wilson Sonsini Goodrich & Rosati (US); Nora Ni Loideain, IALS University of London (UK); Bart van der Sloot, Tilburg University (NL)

Many recent privacy proposals end up being wolves in sheep’s clothing. Sometimes this is because these proposals, on inspection, actually end up being privacy harming data collections systems dressed up as complex privacy enhancing systems; sometimes it’s because systems achieve their privacy aims in ways that box out competitors, and create a false privacy-vs-competition dynamic. This panel discussion will focus on traits common to these false-privacy systems, and features to look out for when evaluating privacy proposals. We’ll focus on reoccurring false trade-offs in this space, including: data vs privacy (systems that claim to improve privacy through additional data collection) and competition vs privacy (e.g., monopolist proposed systems that would harm smaller competitors). Presenters will aim to discuss systems past, current and proposed. Finally, panellists will discuss true privacy preserving alternatives, and how online privacy can be improved without harming users or competition:

- What are traits common to false-privacy systems and what features should be looked out for when evaluating proposals?
- What are the recurring false trade-offs in the space?
- Which systems – past, present and future – might be discussed as relevant?
- What are the true privacy preserving alternatives?

15:30 - COFFEE BREAK

16:00 – JUSTICE 3.0: AI IN AND FOR JUSTICE AND CASE-LAW AS BIG DATA CHALLENGES

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Scuola Superiore Sant’Anna (IT)
Moderator Giovanni Comandé, Scuola Superiore Sant’Anna, Pisa (IT)
Speakers Thibault Douville, Université de Caen (FR); Angelo Dalli, UMNAI (MT); Francesca Toni, Imperial College (UK)

Both the European regulatory landscape and international markets for legal services display a flourishing of initiatives to expand the use of AI and discovery knowledge. A number of products are on the markets while they are outlawed in some countries. Against a backdrop of EU initiatives to foster the re-use of judicial data, the proposed AI regulation exhibits high suspiciousness concerning the use of AI in administering justice and in law enforcement while remains rather silent on the use of the same technologies by private entities. Many of the concerns raised by the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe in 2018 still remain largely unaddressed while judicial data as such begins to be seen as a source of social data for policy analysis with KDD and AI methods and tools. This panel will:

- Explore the suitability of the various technologies to preserve adequate levels of personal data protection and bias prevention without losing effectiveness
- Test the state of art in data and argument mining from judicial data, also for policy
- Consider the ethical constraints needed to steer AI in and for justice
- Provide an overview of the possible challenges emerging from considering case law and legal materials as big, possibly open, data.

17:15 – EMPOWERING THE AI ACT: LIMITS AND OPPORTUNITIES

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Smart Global Governance / EDHEC Augmented Law Institute (FR)
Moderator Gianclaudio Malgieri, EDHEC Augmented Law Institute (FR)
Speakers Adriano Daulisa, Smart Global Governance (FR); Ursula Pahl, BEUC (BE); Vincenzo Tiani, Brussels Privacy Hub (BE), Yordanka Ivanova, DG CNECT (EU)

The AI Act is an incredible innovation in the EU legal scenario. However, both the blacklist and the “high risk” list of AI practices might appear too narrow (the EDPB denounced the lack of protection for biometric identification and emotion recognition) and not not flexible enough for the challenges ahead. This panel aims to address, thus, the current limits but also the opportunities of the AI Act proposal. Possible tools could help to empower the current proposal, e.g.: a more flexible notion of risk, a better consideration of emotion recognition, but also individual rights, including an ex-ante duty of participatory design and development of the AI systems.

- Should the blacklist in the AI Act include also other AI practices (e.g., emotion recognition, commercial manipulation)?
- Should other tools protect individuals too (e.g. participatory design)? How?
- Is the proposed system of “high risk” classification effective, forward-looking and flexible enough?
- Is the AIA well connected to other existing legal frameworks (GDPR, EU Consumer protection law)?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIOROWSKI (EPDS) in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON in Le Village

CPDP2022 PANELS AT AREA 42 PETITE

08:45 – A CYBERSECURITY INCIDENT: WHO YOU GONNA CALL?

Academic ☆☆☆ **Business** ☆☆☆ **Policy** ☆☆☆
Organised by Université du Luxembourg (LU)
Moderator Sandra Schmitz, SnT, Université du Luxembourg (LU)
Speakers Pascal Steichen, securitymadein.lu, European Cybersecurity Competence Centre (ECCC) (LU); Corinna Schulze, SAP (DE); Florian Pennings, Microsoft (BE); Dennis-Kenji Kipker, Hochschule Bremen, Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen (DE)

The Proposal for a revised Network and Information Systems Directive (NIS 2.0 Proposal) encourages Member States to implement a single entry point for all notifications required under the NIS Directive and also under other Union law such as the GDPR and ePrivacy Directive. This panel discusses the organisational and legal requirements for such a “112” single cybersecurity emergency number solution, and whether further harmonization of the various reporting obligations is necessary.

- Is there a necessity to simplify security incident reporting?
- Considering a single cybersecurity emergency number solution, does this require streamlining reporting timeframes and content?
- Do factors such as different protection goals and levels inhibit streamlining?
- Is there a real risk of overreporting in light of the envisaged obligation to report cyber threats and incidents that have the potential to cause harm?

10:00 - COFFEE BREAK

10:30 – ACADEMIC SESSION 1

Academic ☆☆☆☆☆
Organised by CPDP
Moderator Ricardo R. Campos, Goethe-Universität Frankfurt (DE)

- Valeria Ferrari, University of Amsterdam (NL): The money of the present future: the platform imaginary and the empowerment/protection of consumers in EU policymaking on digital payment infrastructures
- Laima Janciute, Vilnius University (LT): The right to preserve the use of cash: innovation, counter-currents, and the protection of privacy

- Ine van Zeeland, Vrije Universiteit Brussel (BE) and Jo Pierson, Vrije Universiteit Brussel (BE): Data Protection Risks in Transitional Times: The Case of European Retail Banks
- Daniel Woods, University of Innsbruck (AT): Quantifying Privacy Harm via Personal Identity Insurance

11:45 – ACADEMIC SESSION 2

- Academic** ☆☆☆☆☆☆
Organised by CPDP
Moderator Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research ISI (DE)
- Katherine Nolan, London School of Economics and Political Science (UK): The role of the individual in data protection law: object, subject, and agent
 - Davide M. Parrilli and Rodrigo Hernández-Ramírez, European University of Lisbon (PT): Enhancing User Privacy through Ethical Design: The Case of Dark Patterns in Cookie Banners
 - Maximilian Hils, Daniel Woods, and Rainer Boehme, Innsbruck University (AT): Conflicting Privacy Preference Signals in the Wild
 - Wenlong Li, University of Birmingham (UK) and Jill Toh, University of Amsterdam (NL): Data Rights ‘in Dutch’: The Promises and Pitfalls of Uber/Ola Judgments in the Era of Digital Worker Resistance

13:00 - LUNCH

14:15 – LIMITING STATE SURVEILLANCE BY MEANS OF CONSTITUTIONAL LAW: POTENTIALS AND LIMITATIONS

- Academic** ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Fraunhofer ISI
Moderator Murat Karaboga, Fraunhofer ISI (DE)
Speakers Christian Gemin, Univ. Kassel (DE); Jane Kilpatrick, Statewatch (UK); Ulf Buermeyer, GFF/EDRi (DE); Michael Kilchling, MPI-CSL (DE)

In its 2010 ruling on data retention, the German Federal Constitutional Court stipulated that the legislature is henceforth obliged to exercise greater restraint when considering new retention obligations or authorizations in view of the totality of the various data collections already in place. From this, the German law professor Alexander Roßnagel derived a government obligation to examine the proportionality of the overall burdens on civil liberties on the basis of an overall consideration of all government surveillance measures (the so-called “surveillance calculus” or “Überwachungs-Gesamtrechnung” in German). According to this interpretation, there is a maximum level of state surveillance that must not be exceeded. For example, once a certain threshold is reached, the legislator would have to exchange one surveillance measure for another, rather than introducing an additional one. This panel will discuss the potential and limitations of such a calculation as well as possible approaches to its implementation.

- How can we record and, especially, assess the different surveillance measures of the various legislators on the EU, national, regional and local level?
- What would be the expected legislative effect: Would the oldest surveillance measure have to be repealed or would the latest never take effect?
- There are also fundamental questions: What would be an acceptable level of surveillance and who determines it?
- Would a surveillance calculus rather lead to a critical control or to legitimisation of (additional) surveillance measures?
- What value could this debate have for the rest of the EU or even beyond? Are there any points of reference in EU law or in the constitutional law of other member states that could prescribe such a ceiling for state surveillance?

15:30 - COFFEE BREAK

16:00 – ACADEMIC SESSION 3

- Academic** ☆☆☆☆☆☆
Organised by CPDP
Moderator Bart Van der Sloot, Tilburg University (NL)

- Suncana Slijepcević, Bruno Škrinjarić and Edo Rajh, The Institute of Economics, Zagreb (HR): Citizens resilience to online privacy violation and use of digital public services (online participation)
- Jorge Pereira Campos, João Gonçalves and Jason Pridmore, Erasmus University Rotterdam (NL): Data Donation as e-Participation: How Citizens Construct the Risks of Donating Personal Data to Smart Cities
- Elisa Orru, University of Freiburg (DE): Preemptive security: the role of ICTs and the regulatory framework. An analysis based on the PNR-Directive
- Hunter Dowart, Future of Privacy Forum (US): Chinese Data Protection in Transition: A Look at Enforceability of Rights and the Role of Courts

17:15 – GOVERNMENT ACCESS TO DATA HELD BY THE PRIVATE SECTOR: HOW CAN DEMOCRACIES SHOW THE WAY?

- Academic** ☆☆ **Business** ☆☆ **Policy** ☆☆
Organised by Georgia Institute of Technology, School of Cybersecurity and Privacy (US)
Moderator Peter Swire, Georgia Institute of Technology, School of Cybersecurity and Privacy (US)
Speakers Théodore Christakis, Université Grenoble Alpes (FR); Ralf Sauer, DG Justice (EU); Samm Sacks, Yale Law School/ New America (US); Georgia Bruce, DCMS (UK)

What set of principles and laws should apply to government access to personal data, including for law enforcement, foreign intelligence, and national security purposes? As framework privacy and data protection laws have spread to most countries in the world, there is considerable uncertainty about how protections apply outside of the commercial sector. In democracies, state power should be exercised under the rule of law, generally including a prominent role for an independent judiciary. Non-democracies have also adopted framework data protection laws, but with uncertainty about how rule of law may apply for government actions. China has now adopted a framework data protection law, but lacks important rule of law institutions. The United States is a democracy with rule of law under its Constitution, but lacks a framework data protection law. Principled discussion about government access thus is emerging as central to geopolitical debates.

- What are the best forums for multi-lateral consideration of these issues of government access?
- What is the difference between “compelled/obliged” access and “direct” access? Does this difference matter when it comes to promoting democratic principles on government access to data held by the private sector?
- What legal rules and principles should apply to a democracy’s efforts to protect its national security through intelligence collection outside of its borders, including toward both allies and adversaries?
- What could we learn from recent developments on these matters, including the EU/US negotiations for a successor to Privacy Shield and the OECD process following the G20 initiative for free data flows with trust?

18:30 – CLOSING REMARKS BY PAUL DE HERT (VUB) AND WOJCIECH WIEWIÓROWSKI (EPDS) in Grande Halle

19:00 – COCKTAIL SPONSORED BY PRIVACY SALON in Le Village

SPONSORS & PARTNERS

     			PLATINUM
      			PREMIER
           			EVENT SPONSORS
                        			EVENT PARTNERS
                           			EVENT PARTNERS
                			MEDIA PARTNERS

INFO, PROGRAM & REGISTRATION: WWW.CPDPCONFERENCES.ORG

Venues: Les Halles de Schaerbeek & Area 42, Brussels, Belgium

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

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